**LICEO SCIENTIFICO STATALE "FILIPPO LUSSANA"**
Via Angelo Maj, 1 – 24121 BERGAMO
☎ 035 237502 Fax: 035 236331 Sito e contatti: www.liceolussana.gov.it
C. F. 80026450165 e-mail: **bgps02000g@istruzione.it**; bgps02000g@pec.istruzione .it

## Il Dirigente scolastico

**Visto** il decreto legislativo 30 giugno 2003, n.196 recante il Codice in materia di protezione di dati personali, e segnatamente gli artt. 33 e ss., nonché l'allegato B del suddetto D.lgs., contenente il Disciplinare tecnico in materia di misure minime di sicurezza;

**Considerato** che il Liceo Scientifico Statale " F. Lussana" è titolare del trattamento di dati personali ai sensi dell'art.28 del d.lgs. n. 196 del 2003;

**Visto** l'obbligo di prevedere ed applicare le misure minime di sicurezza di cui agli artt. 31 e ss. del D.lgs. n.196 del 2003;

**Visto** il Regolamento recante identificazione dei dati sensibili e giudiziari trattati e delle relative operazioni effettuate dal Ministero della Pubblica Istruzione, emanato con Decreto Ministeriale n.305 del 7.12.2006;

**Adotta il**
**DOCUMENTO PROGRAMMATICO SULLA SICUREZZA**

Il presente documento, elaborato al fine di mettere in atto le misure di sicurezza per tutelare i dati personali oggetto di trattamento, fornisce una individuazione dei criteri tecnici ed organizzativi per la protezione delle aree e dei locali interessati a misure di sicurezza e dei criteri per assicurare l'integrità dei dati, da adottare per il trattamento dei dati personali effettuato dal personale del Liceo Scientifico Statale " F. Lussana" il cui legale rappresentante pro-tempore è il Dirigente scolastico Prof.ssa Stefania Maestrini che nel seguito del documento sarà indicato come " titolare". Il presente documento è aggiornato periodicamente ed i termini utilizzati seguono le definizioni riportate all'art.4 del D.lgs 196/2003. Del documento fanno parte integrante le schede allegate al Regolamento del Ministero della Pubblica Istruzione citato nelle premesse.

### 1 Elenco dei trattamenti di dati personali

### 1.1 Finalità

Il trattamento dei dati personali è funzionale al raggiungimento delle finalità di istruzione e di formazione in ambito scolastico, professionale e superiore, con particolare riferimento a quelle svolte anche in forma integrata, ed è quindi di rilevante interesse pubblico, ai sensi degli articoli 20 e 21 del D.lgs 196/2003. Per le sue finalità istituzionali, l'Istituzione scolastica tratta dati personali, sia comuni che sensibili o giudiziari, di studenti, genitori, personale dipendente e fornitori.

### 1.2 Luoghi di tenuta e trattamento dei dati:

I dati su supporto cartaceo sono conservati negli armadi degli uffici: amministrativo, del personale, didattica alunni, nella stanza denominata archivio corrente e nella stanza denominata archivio storico.

I dati acquisiti attraverso il protocollo riservato sono conservati nell'ufficio di Presidenza.

I dati su supporto elettronico sono conservati negli archivi elettronici dei computer di tutti i servizi amministrativi.

(Nella tabella che segue, relativamente ai dati sensibili e giudiziari, nella descrizione sintetica del trattamento, le finalità e le attività svolte, i tipi di dati trattati e le operazioni eseguite sono indicati in modo sintetico e con riferimento alle schede allegate al Regolamento del Ministero della Pubblica

Istruzione citato nelle premesse, con specificazione, per ogni identificativo di trattamento, delle specifiche schede).

# *TABELLA IDENTIFICATIVI DEI TRATTAMENTI*

| ***Id Trattamento*** | ***Descrizione sintetica del trattamento*** <br> ***Finalità perseguita o attività svolta*** |
|---|---|
| **T1** | **Gestione Area Alunni** Relativamente ai dati sensibili e giudiziari:<br>Scheda n. 4 – Attività propedeutiche all'avvio dell'anno scolastico;<br>Scheda n. 5 – Attività educativa, didattica e formativa e di valutazione;<br>Scheda n. 7 – Rapporti Scuola-Famiglie: gestione del contenzioso. |
| **T2** | **Gestione Area Bilancio** |
| **T3** | **Gestione Area Personale**<br>Relativamente ai dati sensibili e giudiziari:<br>Scheda n. 1 – Selezione e reclutamento a TI e TD e gestione del rapporto di lavoro;<br>Scheda n. 2 – Gestione del contenzioso e procedimenti disciplinari;<br>Scheda n. 3 – Organismi collegiali e commissioni istituzionali;<br>Scheda n. 7 – Rapporti Scuola-Famiglie: gestione del contenzioso. |
| **T4** | **Gestione Area Retribuzioni**<br>Relativamente ai dati sensibili e giudiziari:<br>Scheda n. 1 – Selezione e reclutamento a TI e TD e gestione del rapporto di lavoro;<br>Scheda n. 2 – Gestione del contenzioso e procedimenti disciplinari;<br>Scheda n. 3 – Organismi collegiali e commissioni istituzionali; |
| **T5** | **Gestione Fiscale** |
| **T6** | **Gestione Protocollo**<br>Relativamente ai dati sensibili e giudiziari:<br>Tutte le schede allegate al regolamento sul trattamento dei dati sensibili e giudiziari |
| **T7** | **Gestione Sicurezza** |
| **T8** | **Backup e Restore** |

| | |
|---|---|
| **T9** | **Gestione Protocollo e corrispondenza riservata**<br>Relativamente ai dati sensibili e giudiziari:<br>Tutte le schede allegate al regolamento sul trattamento dei dati sensibili e giudiziari |
| **T10** | **Gestione della posta elettronica** |
| **T11** | **Gestione Scioperi del Personale dipendente**<br>Relativamente ai dati sensibili e giudiziari:<br>Scheda n. 1 – Selezione e reclutamento a TI e TD e gestione del rapporto di lavoro; |
| **T12** | **Gestione Anagrafe delle prestazioni** |
| **T13** | **Invio documenti tramite Entratel e DM10** |
| **T14** | **Gestione Pre96** |
| **T15** | **Gestione INPS** |
| **T16** | **Gestione con Suite Microsoft Office comunicazione** |
| **T17** | **Gestione Dispostivi dell'infrastruttura tecnologica** |
| **T18** | **Gestione Provvedimenti Disciplinari alunni**<br>Relativamente ai dati sensibili e giudiziari:<br>Scheda n. 4 – Attività propedeutiche all'avvio dell'anno scolastico;<br>Scheda n. 5 – Attività educativa, didattica e formativa e di valutazione;<br>Scheda n. 7 – Rapporti Scuola-Famiglie: gestione del contenzioso. |
| **T19** | **Gestione Graduatorie e supplenze** |
| **T20** | **Gestione del personale** |
| **T21** | **Gestione III^ Area e Contratti prestazione** |
| **T22** | **Gestione Trattative sindacali**<br>Relativamente ai dati sensibili e giudiziari:<br>Scheda n. 3 – Organismi collegiali e commissioni istituzionali; |
| **T23** | **Gestione Archivio cartaceo storico** |
| **T24** | **Gestione Assistenza e manutenzione hardware** |
| **T25** | **Gestione titolario Generale** |
| **T26** | **Gestione Riproduzione e notifica documenti** |

| | |
|---|---|
| **T27** | **Gestione Atti cartacei amministrativi** |
| **T28** | **Gestione Inventario e Fornitori di beni e servizi** |

**2 Distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati**

Le misure indicate nel presente documento sono relative alla sede centrale dell'Istituzione scolastica.

Il titolare del trattamento ha designato, ai sensi dell'art. 29 D.lgs 196/2003, con atto scritto contenente analitiche istruzioni relative ai compiti affidati, il responsabile del trattamento nella persona del DSGA Dott.ssa D'Amato Anna Maria.

Il responsabile del trattamento ha provveduto, sulla base della lettera di designazione e delle disposizione dell'art.30, ad individuare gli incaricati del trattamento dei dati personali appartenenti ai profili professionali del personale ATA; ha conferito agli stessi l'incarico con atto scritto contenente puntuali istruzioni relative agli ambiti di trattamento consentiti, corredato da linee guida e con allegate le schede relative al trattamento dei dati sensibili e giudiziari.
Il Responsabile del trattamento ha provveduto altresì a individuare, nominare e incaricare per iscritto un incaricato della gestione e della manutenzione degli strumenti elettronici, un incaricato della custodia delle copie delle credenziali e un incaricato delle copie di sicurezza delle banche dati ai quali sono state fornite puntuali istruzioni relative ai compiti da svolgere. Il titolare ha direttamente provveduto ad individuare e incaricare il personale docente con atto che fornisce le istruzioni necessarie. I singoli incaricati, che hanno rilasciato ricevuta della avvenuta consegna della lettera di incarico, sono stati informati che l'ambito dei trattamenti autorizzati è suscettibile di aggiornamento periodico e che sono tenuti ad attenersi al divieto di comunicazione e diffusione dei dati trattati nel corso dell'incarico, anche per il tempo successivo alla sua cessazione, senza limiti temporali.
La comunicazione dei soggetti previsti dal D.lgs 196/2003 è avvenuta attraverso la pubblicazione all'albo della scuola dell'organigramma della scuola e delle responsabilità.
A tutti gli incaricati del trattamento di dati mediante strumento elettronico sono state conferite credenziali di autenticazioni (art.34, comma 1, lett.b) mediante parola chiave. Agli incaricati sono state fornite puntuali indicazioni per la modifica della parola chiave ogni tre mesi.

**3 Analisi dei rischi che incombono sui dati**

La ricognizione e l'analisi dei rischi, che potrebbero comportare una distruzione, sottrazione, perdita, trattamento abusivo dei dati, di origine dolosa, colposa, ovvero meramente fortuita, in grado di recare pregiudizio ai dati personali trattati, è stata riportata nelle tabelle che seguono nelle quali gli eventi sono stati suddivisi in tre categorie:

**1) Comportamenti degli operatori**

Sottrazione di credenziali di autenticazione; carenza di consapevolezza, disattenzione o incuria; comportamenti sleali o fraudolenti; errori materiali.

**2) Eventi relativi agli strumenti**

Danno arrecato da virus informatici o di programmi suscettibili di recare danno; spamming o tecniche di sabotaggio; malfunzionamento, indisponibilità o usura degli strumenti; accessi esterni non autorizzati; intercettazione di informazioni in rete.

**3) Eventi relativi al contesto fisico-ambientale**.

Accessi non autorizzati a locali ad accesso ristretto; eventi distruttivi naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, ecc) nonché dolosi,

accidentali o dovuti ad incuria; guasto ai sistemi complementari (impianto elettrico, riscaldamento, ecc); errori umani nella gestione della sicurezza fisica.

I suddetti rischi sono stati ripartiti in classi di gravità, tenendo conto della concreta possibilità di realizzazione, adottando la seguente scansione:

**Alta - Bassa - Molto Elevata - Media - Medio-Alta - Medio-Bassa**

La tabella seguente sintetizza i principali eventi potenzialmente dannosi per la sicurezza dei dati, valutandone l'impatto sulla sicurezza. le possibili conseguenze e stimandone la gravità, ponendoli altresì in correlazione con le misure di sicurezza previste.

**Tabella 3 – Analisi dei rischi (regola 19.3 del disciplinare tecnico)**

| | ***Id Rischio*** | ***Rischi*** | ***Si/No*** | ***Descrizione dell'impatto sulla sicurezza (gravità alta/media/ bassa)*** |
|---|---|---|---|---|
| **Comportamento degli operatori** | **R1** | **Sottrazione di credenziali di autenticazione.** | **Si** | **Alta** |
| | **R2** | **Carenza di consapevolezza, disattenzione o incuria.** | **Si** | **Media** |
| | **R3** | **Comportamenti sleali o fraudolenti.** | **Si** | **Bassa** |
| | **R4** | **Errore materiale.** | **Si** | **Media** |
| **Eventi relativi agli strumenti** | **R5** | **Azione di *virus* informatici o di programmi suscettibili di recare danno.** | **Si** | **Alta** |
| | **R6** | ***Spamming* o tecniche di sabotaggio.** | **Si** | **Alta** |
| | **R7** | **Malfunzionamento, indisponibilità o degrado degli strumenti.** | **Si** | **Media** |
| | **R8** | **Accessi esterni non autorizzati.** | **Si** | **Media** |
| | **R9** | **Intercettazione di informazioni in rete.** | **Si** | **Media** |
| **Eventi relativi al contesto** | **R10** | **Accessi non autorizzati a locali/reparti ad accesso ristretto.** | **Si** | **Bassa** |
| | **R11** | **Eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, ecc,) nonché dolosi, accidentali o dovuti ad incuria.** | **Si** | **Media** |

| | | | | |
|---|---|---|---|---|
| | **R12** | **Guasto ai sistemi complementari (impianto elettrico, climatizzazione, ecc.).** | **Si** | **Media** |
| | **R13** | **Errori umani nella gestione della sicurezza fisica.** | **Si** | **Media** |

## 4 Misure da adottare per garantire l'integrità e la disponibilità dei dati, non che la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità

Contro i rischi d'intrusione i locali della sede centrale, unica sede nella quale sono detenuti dati soggetti a protezione, sono dotati di impianto d'allarme a sensori infrarossi, attivabile mediante digitazione d'un codice consegnato al personale dipendente. E' stata disposta l'attivazione dell'allarme al termine dell'orario di lavoro.
Le aree contenenti dati in supporto cartaceo (archivio e mobili contenenti documentazione contabili dei dipendenti e degli alunni) sono ubicate in modo tale che ciascun addetto possa rilevare a vista e impedire il tentativo di accesso da parte di persone estranee.
Sono state impartite disposizioni affinché, in assenza del personale, le stanze rimangano chiuse e le chiavi siano custodite dal personale collaboratore scolastico in servizio addetto alla vigilanza che, al termine del servizio, provvederà al deposito delle chiavi nell'apposito contenitore.
L'ubicazione di stampanti ed apparecchio telefax tradizionale non consente ad estranei di leggere od asportare eventualmente documenti non ancora prelevati dal personale.

Di seguito si illustrano le norme applicate per garantire la sicurezza e l'integrità dei dati per:

- *Computer e supporti informatici*: I computer risultano quasi tutti sollevati da terra, in modo da evitare eventuali perdite di dati dovuti ad allagamenti; il server è installato in un rack e collegato ad un gruppo di continuità che consente di escludere la perdita di dati derivanti da sbalzi di tensione o di interruzione di corrente elettrica. L'integrità dei dati sul server amministrativo è garantita da una doppia procedura di backup: la prima avviene in automatico con apposito software che giornalmente opera il salvataggio di una copia dei dati su un apposito disco installato nel PC della DSGA e nel PC WKS10, localizzati in due stanze diverse e non direttamente accessibili dalla sala server. Tali cartelle sono accessibili al solo utente amministratore. Il server della rete amministrativa viene protetto da password per impedire al personale non autorizzato l'accesso alla rete amministrativa. La password è assegnata e riportata su un apposito foglio conservato nella cassaforte collocata nell'ufficio del DSGA. L'introduzione delle password inibisce ad estranei l'uso dei personal computer.
- Per l'invio di messaggi e-mail a più destinatari, sono state fornite al personale istruzioni affinché quale destinatario venga sempre indicata la scuola con l'indirizzo e-mail e in CCN i destinatari, in modo che non possano essere individuati gli indirizzi e-mail degli altri destinatari attraverso la funzione di proprietà.
- Per quanto riguarda infine l'obbligo previsto dalle misure minime sulla sicurezza di cui all'allegato B del codice della privacy, i computer sono dotati di programma antivirus. Il programma viene aggiornato sotto la responsabilità del titolare del trattamento a cadenza semestrale e che consente di rilevare immediatamente all'apertura di un file la presenza di un virus. La base dati dell'antivirus viene aggiornata in automatico ogni 6 ore.
- *Supporti cartacei:* relativamente ai supporti cartacei sono state impartite dettagliate istruzioni a tutto il personale al momento dell'affidamento dell'incarico. (vedi lettere di individuazione degli incaricati del trattamento dei dati e Linee Guida allegate)
- *Gestione della privacy e trattamento dei dati raccolti attraverso il sito Web*

Si rimanda al link Privacy pubblicato sul sito: www.liceolussana.gov.it .

## 5 Descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento

Al fine di garantire il ripristino dei dati in seguito a distruzione o danneggiamento, l'istituzione scolastica dispone di idonee procedure di salvataggio periodico (backup) che consistono nell'utilizzo dell'apposito software di backup del programma di gestione amministrativo il quale crea in automatico una copia compressa dei dati, archiviandoli in un'apposita cartella del server, e successivamente spostati come per i dati in altri due dischi localizzati in stanze diverse.

**Tabella 5.1 – Criteri e procedure per il ripristino della disponibilità dei dati (regola 19.5 del disciplinare tecnico)**

| Ripristino | | |
|---|---|---|
| ***Banca dati / archivio dati*** | ***Criteri e procedure per il salvataggio e il ripristino dei dati*** | ***Pianificazione delle prove di ripristino*** |
| **DATABASE ARGO** | **In automatico con il software di gestione amministrativo**<br><br>**ARGO-SISSI-INFOSCHOOL -CLESSIDRA con cadenza giornaliera** | **Annuale** |
| **Documenti di Office application** | **In automatico con apposito software a cadenza giornaliera** | **Non necessaria** |
| **Documenti Posta elettronica** | **Le email sono mantenute in backup dai rispettivi provider di posta elettronica.** | **Non necessaria** |

**Tabella 5.2 – Criteri e procedure per il salvataggio dei dati (regola 19.5 del disciplinare tecnico)**

| ***Salvataggio*** | | | |
|---|---|---|---|
| ***Banca dati*** | ***Criteri e procedure per il salvataggio*** | ***Luogo di custodia delle copie*** | ***Struttura o persona incaricata del salvataggio*** |
| **Server** | **Software applicativo ARGO-SISSI-INFOSCHOOL-CLESSIDRA automatizzato**<br><br>**Supporti di bachup in digitale.** | ***Uffici Amministrativi*** | **Amministratore di Sistema** |

## 6 Previsione di interventi formativi degli incaricati del trattamento

Gli interventi formativi saranno programmati nell'ambito del piano di formazione e aggiornamento del personale, per rendere gli incaricati del trattamento edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. Saranno previste idonee attività di formazione in occasione di innovazioni e/o modifiche delle norme e in relazione allo sviluppo scientifico/tecnologico dei mezzi e dei sistemi di protezione.

La formazione verrà altresì programmata al momento dell'ingresso in servizio, in occasione di cambiamenti di mansioni o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali. L'incarico al trattamento dei dati contiene, oltre alle istruzioni date dal responsabile, anche le linee guida per il trattamento dei dati, le informazioni relative al significato dei termini e le schede allegate al Regolamento recante identificazione dei dati sensibili e giudiziari trattati e delle relative operazioni effettuate dal Ministero della Pubblica Istruzione. Gli incaricati parteciperanno alla riunione annuale per la verifica e la revisione del documento programmatico per la sicurezza. Verrà valutata l'eventuale partecipazione del personale della scuola alle iniziative formative organizzate dall'USR per la Lombardia.

**Tabella 6 – Pianificazione degli interventi formativi previsti (regola 19.6 del disciplinare tecnico)**

| ***Descrizione sintetica degli interventi formativi*** | ***Classi di incarico o tipologie di incaricati interessati*** | ***Tempi previsti*** |
|---|---|---|
| Attuazione delle norme sulla riservatezza dei dati personali – Acquisizione di competenze giuridiche e di organizzazione scolastica – Responsabilità dei docenti nel trattamento dei dati personali con riferimento al REGOLAMENTO sul trattamento dei dati sensibili e giudiziari | Docenti incaricati del trattamento dei dati personali | Da definire |
| Miglioramento dell'attuazione delle norme sulla riservatezza dei dati personali nella scuola | Personale ATA della scuola | Da definire |

## 7 Individuazione dei criteri da adottare per la cifratura o per la separazione dei dati personali idonei a rivelare lo stato di salute e la vita sessuale (Regola 19.8 del disciplinare tecnico)

L'istituzione scolastica ha messo in atto particolari misure di protezione nell'archiviazione dei dati personali idonei a rivelare lo stato di salute, conservandoli sempre in busta chiusa, inserita all'interno del fascicolo personale.

## 9 Conclusioni

Il presente documento sarà tempestivamente aggiornato nel caso di sostituzione di attrezzature o di cambiamenti nella disposizione degli spazi di lavoro e, in ogni caso, entro il 31 marzo di ciascun anno.

Agli incaricati del trattamento è stata data informazione circa il contenuto del presente documento, attraverso la consegna di una copia , nella quale si dà atto della comunicazione dell'obbligo di uniformarsi al documento.
Il responsabile del trattamento è tenuto a vigilare sull'osservanza delle disposizioni stesse da parte degli incaricati e ad emanare ulteriori disposizioni relative alla gestione della sicurezza dei dati.

Il presente documento sarà illustrato nel corso di riunioni, nel rispetto delle disposizioni del D.Lgs 196/03, che prevede l'elaborazione di un piano di formazione per rendere edotti gli incaricati del trattamento dei rischi individuati e dei modi per prevenire i danni.

In occasione delle riunioni, che saranno successivamente previste per la formazione, si provvederà anche alla valutazione ed alla revisione delle misure di sicurezza.

Le attività di formazione del personale incaricato e di revisione del presente documento verranno annotate in apposito registro verbale tenuto dal Responsabile del trattamento.

Il presente documento verrà illustrato ai docenti in sede di riunione del Collegio Docenti, con particolare riferimento a quanto attiene alle documentazioni ed ai dati personali che vengono consegnati agli stessi e alle istruzioni date ai docenti incaricati del trattamento dei dati.

Bergamo, 31 marzo 2017

Il titolare del trattamento
IL DIRIGENTE SCOLASTICO
Prof.ssa Stefania Maestrini

Documento informatico firmato digitalmente ai sensi del D. Lgs. 82/2005 s.m.i. e norme collegate, il quale sostituisce il documento cartaceo e la firma autografa