ISTITUTO COMPRENSIVO SAMPIERDARENA
PIAZZA DEL MONASTERO 6, GENOVA
***Tel.* 010-936389 - *fax* 010-2344335**
geic85100e@istruzione.it - geic85100e@pec.istruzione.it
www.icsampierdarena.edu.it – C.F. 95159930106

GDPR - EU General Data Protection Regulation
Regolamento Europeo 2016/679
in materia di protezione dei dati personali

GDPR

Registro dei Trattamenti

Ai sensi dell'Art. 30 del R.E. 2016/679

Data Agg.to
30.04.2025

Il Dirigente scolastico

Visto il regolamento UE 2016/679, noto anche come GDPR (General Data Protection Regulation), relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati;

Visto il decreto legislativo 7b dicembre 2006, n. 305 – "Regolamento recante identificazione dei dati sensibili e giudiziari trattati e delle relative operazioni effettuate dal Ministero della Pubblica Istruzione, in attuazione degli artt. 20 e 21 del D.Lgs del 30 giugno 2003, n.196, recante il Codice in materia di protezione di dati personali;

Visto il Decreto Legislativo 10 agosto 2018 n. 101 recante le Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)

Visto l'art. 30 del Regolamento UE 2016/679 GDPR

adotta il seguente **Registro dei Trattamenti,** allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno dell'Istituto Scolastico - indispensabile per ogni valutazione e analisi del rischio, che contiene le informazioni relative a: dati del titolare, finalità del trattamento, categorie degli interessati e dei dati trattati, categorie dei destinatari, misure di sicurezza tecniche ed organizzative.

1. NOME E DATI DEL TITOLARE DEL TRATTAMENTO

IL TITOLARE DEL TRATTAMENTO:
ISTITUTO COMPRENSIVO SAMPIERDARENA – Piazza del Monastero. 6 – 16149 Sampierdarena GE
Tel. **010-936389 -** ***fax*** **010-2344335**
geic85100e@istruzione.it - geic85100e@pec.istruzione.it

Legale Rappresentante
Prof.ssa Sara Bandini
C.F. BNDSRA72D44I693U

2. INDICAZIONI RELATIVE AI DATI TRATTATI

In questa parte del documento vengono fornite informazioni essenziali in merito ai dati personali trattati, con riferimento alla natura ed alla classificazione;

NATURA DEI DATI TRATTATI
La natura dei dati soggetti al trattamento da parte della scuola è la seguente:

- Documentazioni complete riguardanti gli alunni, relativi al corso di studi, alla presenza di handicap, alla certificazione dell'idoneità alla pratica sportiva non agonistica, alla scelta dell'insegnamento della religione cattolica, all'esito di scrutini, esami, piani educativi individualizzati differenziati;
- Documenti prodotti dalle famiglie anche riguardanti la certificazione della situazione patrimoniale e delle condizioni economiche;
- Documentazione riguardante il personale docente e non docente anche con elementi di individuazione di appartenenza sindacale, stato di salute, anche di congiunti per i quali vengono richiesti benefici previsti da particolari norme, allo stato di servizio, alla retribuzione, alle eventuali pratiche disciplinari;
- Dati per gestire le negoziazioni e le relative modalità di pagamento per la fornitura di beni e servizi
- Dati contabili e fiscali

TIPO DI DATI

Sulla scorta delle precisazioni sopra elencate, l'Istituzione Scolastica, sulla base di una prima ricognizione, con riserva della possibilità di procedere a successive integrazioni e/o correzioni dichiara, con riferimento ai destinatari o familiari dei destinatari dell'offerta formativa ovvero del personale coinvolto, a qualunque titolo, nella medesima, o interessato ad essere coinvolto, ovvero di soggetti, a qualsiasi titolo, coinvolti in rapporti negoziali con l'Istituzione Scolastica, o aspiranti ad assumere tale ruolo, di trattare i dati di seguito elencati:

- dati personali comuni (dati anagrafici o identificativi delle persone, indirizzi, recapiti telefonici, codici fiscali, dati bancari, informazioni circa la composizione familiare, la professione esercitata da un determinato soggetto, la sua formazione …);
- dati sensibili (dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute, appartenenza a categorie protette, portatore di handicap, stato di gravidanza, vita sessuale etc.);
- dati giudiziari (provvedimenti sul casellario giudiziale, anagrafe delle sanzioni amministrative dipendenti da reato o dei relativi carichi pendenti, la qualità di imputato o indagato ai sensi degli artt. 60 o 61 del cod. proc. pen., avviso di garanzia, separazioni, affidamento dei figli, etc.).

Nel trattamento dei **dati di natura sensibile e giudiziaria**, così come definiti dall'art. 4 lettere d) ed e), verrà osservato il documento redatto da codesto istituto dal titolo "Regolamento recante identificazione dei dati sensibili e giudiziari trattati e delle relative operazioni effettuate dall'Istituto scolastico".

BANCHE DATI ATTIVATE

Le banche dati attivate sono quelle di seguito riportate:

- Alunni
- Dipendenti
- Protocollo
- Inventario
- Magazzino
- Rapporti con enti ed imprese
- Fornitori
- Bilancio
- Stipendi
- Registro di classe
- Registro degli insegnanti
- Registro infortuni alunni e dipendenti

FINALITÁ PERSEGUITA CON IL TRATTAMENTO DEI DATI

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. Per le sue finalità istituzionali, l'Istituzione scolastica tratta dati personali, sia comuni che sensibili o giudiziari, di studenti, genitori, personale dipendente e fornitori. I trattamenti sono effettuati, anche mediante strumenti elettronici, per le seguenti finalità:

- adempimento agli obblighi di fonte legislativa, nazionale o comunitaria, regolamentare o derivante da atti amministrativi;
- somministrazione dei servizi formativi;
- gestione e formazione del personale, nelle sue varie componenti (docente e non docente, in ruolo presso altri apparati pubblici);
- adempimenti assicurativi;
- tenuta della contabilità;
- gestione delle attività informative curate ai sensi della legge 7 giugno 2000, n.150 contenente la "Disciplina delle attività di informazione e di comunicazione delle pubbliche amministrazioni";
- attività strumentali alle precedenti.

AFFIDAMENTO DEI DATI A TERZI PER IL TRATTAMENTO :
Tutti i dati posseduti dalla scuola vengono trattati esclusivamente presso gli Uffici dell'Istituto e la piattaforma di gestione documentale messa a disposizione di un fornitore esterno e nessuna altra struttura concorre al trattamento dei dati raccolti dall'Istituto. I dati potranno essere comunicati a terzi solo nell'ambito dell'attività istituzionale dell'Istituto e comunque nei casi previsti dalla informativa fornita agli interessati od in seguito ad esplicito consenso espresso dagli stessi.

MODALITÀ DI TRATTAMENTO
I trattamenti sono realizzati prevalentemente:

- negli uffici di direzione e segreteria;
- nell' archivio della sede centrale;
- nelle aule scolastiche;
- sul sito della scuola.

I dati sono trattati con fascicoli e atti cartacei e con strumenti elettronici di elaborazione.
La conservazione ed il trattamento dei dati viene attuata secondo le seguenti modalità:
CARTACEO:
I dati in possesso della scuola sono conservati in locali e armadi dotati di chiusura a chiave ai quali hanno accesso esclusivamente le persone incaricate.
Per i dati sensibili si garantiranno maggiori misure di riservatezza con fascicolazione a parte, con eventuale cifratura o individuando criteri per criptare i dati stessi.
MEDIANTE SISTEMA INFORMATICO:
Il controllo degli accessi alle varie postazioni di lavoro viene effettuato mediante l'istituzione di un sistema di autenticazione che permette l'identificazione indiretta del soggetto autorizzato al trattamento dei dati tramite riconoscimento di una credenziale logica costituita da un codice identificativo associato ad una password.
Il trattamento dei dati avviene attraverso modalità diverse:
strumenti elettronici collegati in rete fra loro e/o mediante collegamenti alla rete intranet, al Sidi, alla rete internet.
Inoltre, l'Istituzione scolastica si serve di software applicativo fornito da AXIOS Italia Service S.r.l.
Attraverso tale software applicativo viene effettuata, altresì, in adempimento degli obblighi di legge, la conservazione a norma del protocollo.
Con riferimento alla gestione dei dati mediante rete ministeriale, l'Istituzione Scolastica declina ogni responsabilità, operando come semplice utente, non essendo in grado di intervenire sulla gestione delle informazioni ivi contenute e gestite.

ELENCO DEI TRATTAMENTI DI DATI PERSONALI
Informazioni di base e descrizione degli strumenti utilizzati:

1		**2**		**3**	**4**	**5**
Identificativo del Trattamento		**Natura dei dati trattati** S G		**Struttura di riferimento**	**Altre strutture concorrenti al trattamento**	**Descrizione degli strumenti utilizzati**
Descrizione Sintetica						
Tr.1	Selezione e reclutamento a tempo indeterminato e determinato e gestione del rapporto di lavoro del personale dipendente etc	S	G	Dirigente Scolastico, DSGA e Segreteria Amministrativa	Collaboratori del D.S., Collaboratori scolastici, RSPP e addetti SPP, Medico Competente (se esiste)	Documenti cartacei, registri e strumenti elettronici, marcatempo collegato al computer
Tr.2	DIPENDENTI E ASSIMILATI Gestione del contenzioso e procedimenti disciplinari	S	G	Dirigente Scolastico, DSGA e Segreteria Amministrativa		Documenti cartacei e strumenti elettronici

Tr.3	Organismi collegiali e commissioni istituzionali	S		Dirigente Scolastico, DSGA e Segreteria Amministrativa	Collaboratori del D.S., Docenti, Collaboratori scolastici, membri esterni organi collegiali	Documenti cartacei e strumenti elettronici
Tr.4	Attività propedeutiche all' avvio dell'anno scolastico	S	G	Dirigente Scolastico, DSGA e Segreteria Amministrativa	Collaboratori del D.S., Docenti, Collaboratori scolastici,	Documenti cartacei, registri e strumenti elettronici
Tr.5	Attività educativa, didattica e formativa, di valutazione	S	G	Dirigente Scolastico, DSGA e Segreteria Amministrativa	Collaboratori del D.S., Docenti, Collaboratori scolastici, membri esterni organi collegiali	Documenti cartacei, registri e strumenti elettronici
Tr.6	Scuole non statali (OPZIONALE, a seconda delle competenze del Dirigente)	S	G	Dirigente Scolastico, DSGA e Segreteria Amministrativa		Documenti cartacei, registri e strumenti elettronici
Tr.7	Rapporti scuola – famiglie : gestione del contenzioso	S	G	Dirigente Scolastico, DSGA e Segreteria Amministrativa Docenti,		Documenti cartacei e strumenti elettronici
Tr.8	Fornitori e clienti			Dirigente Scolastico, DSGA e Segreteria Amministrativa	Collaboratori del D.S., Docenti nelle commissioni, Membri di organi Collegiali, Collaboratori scolastici	Documenti cartacei e strumenti elettronici
Tr.9	Gestione finanziaria e contabile			Dirigente Scolastico, DSGA e Segreteria Amministrativa	Collaboratori del D.S.	Documenti cartacei e strumenti elettronici
Tr.10	Gestione Istituzionale			Dirigente Scolastico, DSGA e Segreteria Amministrativa	Collaboratori del D.S.	Documenti cartacei e strumenti elettronici
Tr.11	Gestione sito web dell'istituto			Dirigente Scolastico, Incaricati sito web	Azienda esterna	Documenti cartacei e strumenti elettronici

3. STRUTTURA ORGANIZZATIVA FUNZIONALE AL TRATTAMENTO DATI

Si riporta di seguito una sintetica descrizione della struttura organizzativa funzionale al trattamento dei dati con i riferimenti agli incarichi conferiti, ai trattamenti operati ed alle relative responsabilità:

Il Dirigente, in quanto Legale Rappresentante della istituzione Scolastica, è il TITOLARE del Trattamento dei dai personali.

Ai sensi dell'art. 4 del Regolamento UE 2016/679, il Titolare è colui che tratta i dati senza ricevere istruzioni da altri e che decide quali dati, oltre che perché e come, devono essere trattati. Il titolare è colui che decide, ma è anche il Responsabile che risponde delle eventuali conseguenze dei trattamenti effettuati. È questo il principio di **responsabilizzazione** che chiede al titolare del trattamento di mettere in atto misure tecniche e organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al Regolamento. Poiché l'attività di protezione delle persone muta in relazione ai luoghi e ai tempi, il principio di responsabilizzazione comporta anche che il titolare dimostri di essersi continuativamente preoccupato di adottare nel tempo le misure di risposta adeguata. Quella del titolare è una responsabilità che si assume direttamente il dirigente scolastico nel suo ruolo di rappresentante legale e non è quindi soggetto a nomina.

L'art. 4 sopra richiamato individua anche un altro soggetto di rilevante importanza nell'ambito del Trattamento dei dati personali. Si tratta del **Responsabile Protezione Dati (RPD) o Data Protection Officer (DPO)**.
Il Regolamento UE dispone che il titolare del trattamento di una pubblica amministrazione deve provvedere alla nomina di un Responsabile Protezione Dati (RPD) o Data Protection officer (DPO), figura di alto livello professionale con idonee competenze giuridiche, informatiche, di risk management e di analisi dei processi, che deve essere coinvolta in tutte le questioni inerenti alla protezione dei dati personali.

Il Regolamento UE riconosce al RPD funzioni consultive, di vigilanza e di controllo attraverso le seguenti azioni:

➢ "fornire assistenza" (considerando 97 GDPR) e consulenza al designante in condizioni di assoluta autonomia e indipendenza (cfr. spec. art. 38 commi 3 e 6 GDPR);

➢ verificare l'applicazione e l'attuazione sia delle norme sia delle politiche dettate dal designante relativamente al trattamento dei dati personali (cfr. art. 39 c.1, lett. b);

➢ fungere da interlocutore dell'Autorità Garante e degli interessati (cfr. art. 39 e 38 c. 4);

➢ "sorvegliare l'osservanza" di tutte le norme e delle politiche del designante in ordine al trattamento dei dati personali "compresi l'attribuzione delle responsabilità e la sensibilizzazione del personale che partecipa ai trattamenti e alle connesse attività di controllo" (art. 39 c.1, lett. b).

Il Responsabile Protezione Dati può anche essere una figura interna all'amministrazione anche se ciò accade molto di rado nelle istituzioni scolastiche a causa delle competenze necessarie e dei possibili conflitti di interessi o di mancanza di autonomia che possono riscontrarsi in figure interne all'amministrazione.
L'assunzione dell'incarico di RPD/DPO deve essere formalizzata con un contratto e i dati di contatto del proprio RPD/DPO devono essere comunicati al Garante privacy attraverso il link:
https://servizi.gpdp.it/comunicazionerpd/s/scelta-auth

Frequenza aggiornamento del contratto: tempestiva alla scadenza del contratto stesso (che può anche essere pluriennale).

RPD/DPO per l'I.C. Sampierdarena è VARGIU Scuola S.r.l. - Referente: Antonio Vargiu.

A tutti i Preposti destinati al trattamento di dati mediante strumento elettronico, vengono conferite credenziali di autenticazioni mediante parola chiave. Con atto allegato al presente documento sono stati designati i preposti alla custodia delle parole chiave, credenziali di autenticazione, nonché della funzione di verifica del loro aggiornamento periodico ovvero della corretta utilizzazione. Le suddette credenziali sono disattivate automaticamente dal gestore della rete periodicamente, ovvero in tutti i casi di mancata utilizzazione per almeno 6 mesi. Al fine di meglio precisare la suddetta ripartizione delle funzioni si rinvia alla tabella seguente:

ASSISTENTI AMMINISTRATIVI

Struttura deputata al trattamento	*Incaricato*	*Trattamenti operati dalla struttura*	*Compiti della struttura*
Segreteria DIDATTICA Protocollo Archivio		**Trattamenti strumentali allo svolgimento dei compiti istituzionali:** gestione della corrispondenza ricevuta ed inviata dal Dirigente Scolastico; tenuta del protocollo generale	Acquisizione e caricamento dei dati, consultazione, stampa, comunicazione a terzi, manutenzione Tecnica dei

Servizi inerenti offerta formativa Servizi strumentali agli organi collegiali Servizi inerenti la gestione amministrativa		con conseguente registrazione della posta e delle comunicazioni di ufficio in entrata e in uscita **Trattamenti strumentali alla predisposizione e concreta erogazione dell'offerta formativa:** raccolta delle domande di iscrizione; condizioni sanitarie ed economiche dei destinatari dell'offerta formativa, documentazione concernente opzioni per insegnamenti facoltativi, dati inerenti profili sanitari o relativi al nucleo familiare dei destinatari dell'offerta formativa, per il riconoscimento di attività di sostegno in ragione di situazioni di disagio, sociale, economico o familiare, registri relativi alle presenze presso l'Istituzione Scolastica **Trattamenti strumentali alle attività degli organi collegiali ed attività connesse ai rapporti con organi pubblici:** composizione degli organi collegiali rappresentativi della comunità servita dall'offerta formativa, convocazione degli organi, raccolta delle delibere, raccolta degli atti concertati con altre istituzioni pubbliche. Gestione dei beni scolastici.	programmi utilizzati nel trattamento, gestione tecnica operativa della base dati (salvataggi, ripristini, ecc.)
Segreteria AMMINISTRATIVA Gestione del personale Servizi amministrativi		**Trattamenti strumentali allo svolgimento dei compiti istituzionali, in materia di selezione ed amministrazione del personale:** registrazione delle presenze presso l'Istituzione Scolastica, assenze per malattia, esigenze familiari, espletamento funzioni politiche o sindacali etc.; aspetti economici e previdenziali: paghe contributi, etc.; raccolta di curricula riguardo a soggetti interessati all'espletamento di funzioni docenti **Trattamenti**	Acquisizione e caricamento dei dati, consultazione, stampa, comunicazione a terzi, manutenzione tecnica dei programmi utilizzati nel trattamento, gestione tecnica operativa della base dati (salvataggi, ripristini, ecc.)

		strumentali allo svolgimento dei compiti di gestione amministrativa: tenuta dei dati connessi all'espletamento di procedimenti amministrativi, attività contrattuale, procedure di bilancio	

COLLABORATORI SCOLASTICI

I Collaboratori Scolastici, nei loro specifici incarichi o nelle loro mansioni generali previsti dal C.C.N.L. e dalla Contrattazione di Istituto nell'area specifica di appartenenza (accoglienza e sorveglianza nei confronti degli alunni, ausilio materiale nei confronti degli alunni in situazione di difficoltà, custodia e sorveglianza nei locali scolastici, vigilanza nei confronti del pubblico evitando ed inibendo l'intrusione di persone estranee, collaborazione con i docenti e con il personale di segreteria, pulizia dei locali), osserveranno la massima privacy, evitando di diffondere notizie che devono restare private, in particolare quando ricevono, per essere distribuite, circolari interne e comunicazioni in visione al personale docente.

DOCENTI

I docenti a tempo indeterminato o determinato e tutte le altre unità di personale che a qualunque titolo hanno rapporto di lavoro anche occasionale (stipule di contratti o convenzioni) con l'Istituzione Scolastica eviteranno di diffondere notizie che resteranno segrete sia per quanto attiene i dati personali comuni, sia per i dati sensibili che hanno acquisito in virtù del loro ufficio. Il docente, per la sfera di competenza, rientra nell'ambito dei soggetti indicati dall'art. 29 del Regolamento UE 2016/679 che agiscono, nell'ambito del trattamento dei dati personali, sotto la diretta autorità del Titolare del trattamento sia per le categorie di dati cui può accedere, sia per la tipologia di trattamento e vincoli specifici ai sensi dell'art. 4 del Codice, sia per le istruzioni in merito ai soggetti cui i dati possono essere comunicati o diffusi.

I dati trattati dai docenti si rinvengono nei registri dei verbali degli OO.CC., nel registro elettronico, nelle diagnosi funzionali per la situazione di handicap, in eventuali certificati medici, etc. Il trattamento dei dati da parte dei docenti è definito puntualmente da norme di legge.

SITO WEB, ALBO ON LINE

Il personale docente e gli alunni che si occupano del sito web della scuola e il personale amministrativo che si occupa dell'albo on line eviteranno di diffondere notizie che resteranno segrete sia per quanto attiene i dati personali comuni, sia per i dati sensibili che hanno acquisito in virtù del loro ufficio. Entrambe le figure rientrano nell'ambito dei soggetti indicati dall'art. 29 del Regolamento UE 2016/679 che agiscono, nell'ambito del trattamento dei dati personali, sotto la diretta autorità del Titolare del trattamento sia per le categorie di dati cui possono accedere, sia per la tipologia di trattamento e vincoli specifici ai sensi dell'art.4 del Codice, sia per le istruzioni in merito ai soggetti cui i dati possono essere comunicati o diffusi.

Tale personale riceverà specifica informazione/formazione da parte del Titolare del trattamento circa gli specifici doveri e gli adempimenti cui sono tenuti in ragione del loro ufficio, della riservatezza che si deve ai dati che trattano per il fatto di essere dipendenti di questa pubblica Istituzione Scolastica. Ad essi sarà consegnato una copia della normativa che riguarda la sicurezza del trattamento dei dati in vigore al momento della nomina. Tale nomina è a tempo indeterminato, decade per revoca, o con il venir meno dei compiti che giustificavano il trattamento

4. ANALISI DEI RISCHI INCOMBENTI SUI DATI

L'Istituzione Scolastica ha proceduto ad una ricognizione dei rischi che potrebbero comportare la distruzione, sottrazione, perdita, trattamento abusivo dei dati di origine dolosa, colposa, ovvero meramente fortuita, in grado di recare pregiudizio ai dati personali trattati.

Le fonti di rischio sono state accorpate in:

1) Comportamenti degli operatori

Sottrazione di credenziali di autenticazione; comportamenti imperiti, imprudenti o negligenti dei soggetti legittimati al trattamento dei dati; comportamenti dolosi dei soggetti legittimati; errori materiali.

2) Eventi relativi agli strumenti
Danno arrecato da virus informatici e/o da hackers, mediante interventi precedenti all'aggiornamento degli strumenti di contrasto attivati (software e firewall), spamming o tecniche di sabotaggio. Malfunzionamento, indisponibilità o usura fisica degli strumenti. Accessi abusivi negli strumenti elettronici. Intercettazione dei dati in occasione di trasmissione in rete.
3) Eventi relativi al contesto fisico-ambientale.
Distruzione o perdita di dati in conseguenza di eventi incontrollabili (terremoto) ovvero, seppur astrattamente preventivabili (incendi o allagamenti) di origine fortuita, dolosa o colposa, per i quali non è possibile apprestare cautele. Guasti a sistemi complementari, quale la mancata erogazione di energia elettrica per lunghi periodi di tempo, in grado di pregiudicare la climatizzazione dei locali. Furto o danneggiamento degli strumenti elettronici di trattamento dei dati, in orario diverso da quello di lavoro. Accesso non autorizzato da parte di terzi – interni o esterni all'istituzione scolastica – mediante uso abusivo di credenziali di autenticazione, in funzione di danneggiamento o sottrazione dei dati. Errori umani nell'attivazione degli strumenti di protezione.
I suddetti rischi sono **stati ripartiti in classi di gravità, tenendo conto** della concreta possibilità di realizzazione presso l'istituzione scolastica, adottando la seguente scansione:
A= alto B = basso EE = molto elevato M = medio MA = medio-alto MB = medio-basso
La tabella seguente sintetizza i principali eventi potenzialmente dannosi per la sicurezza dei dati, valutandone le possibili conseguenze e stimandone la gravità, ponendoli altresì in correlazione con le misure di sicurezza previste.

Analisi dei rischi

EVENTO	**IMPATTO SULLA SICUREZZA DEI DATI**			**RIF. MISURE DI AZIONE**
	DESCRIZIONE		**GRAVITA' STIMATA**	
COMPORTAMENTI DEGLI OPERATORI	Furto di credenziali di autenticazione	Accesso altrui non autorizzato	M	Vigilanza sul rispetto delle istruzioni impartite
	Carenza di consapevolezza, disattenzione o incuria	Dispersione, perdita e accesso altrui non autorizzato	M	Formazione e flusso continuo di informazione
	Comportamenti sleali o fraudolenti	Dispersione, perdita e accesso altrui non autorizzato	M	Vigilanza sul rispetto delle istruzioni impartite
	Errore materiale	Dispersione, perdita e accesso altrui non autorizzato	M	Vigilanza sul rispetto delle istruzioni impartite, formazione e flusso continuo di informazione
EVENTI RELATIVI AGLI STRUMENTI	Azione di virus informatici o di codici malefici	Perdita o alterazione, anche irreversibile, di dati, di programmi e di elaboratori;	EE	Adozione di idonei dispositivi di protezione: software - firewall
	Spamming o altre tecniche di sabotaggio	Perdita o alterazione, anche irreversibile, di dati, di programmi e di	EE	Adozione di idonei dispositivi di protezione: software - firewall

		elaboratori; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi		
	Malfunzionamento, indisponibilità o degrado degli strumenti	Perdita o alterazione, anche irreversibile, di dati, di programmi e di elaboratori; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	MA	Assistenza e manutenzione continua degli elaboratori e dei programmi; ricambio periodico
	Accessi esterni non autorizzati	Dispersione, perdita o alterazione, anche irreversibile, di dati, nonché manomissione di programmi e di elaboratori; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	MA	Adozione di idonei dispositivi di protezione: password
	Intercettazione di informazioni in rete	Dispersione di dati; accesso altrui non autorizzato	MA	Adozione di idonei dispositivi di protezione: firewall
EVENTI RELATIVI AL CONTESTO	Accessi non autorizzati a locali/reparti ad accesso ristretto	Dispersione, perdita o alterazione, anche irreversibile, di dati, nonché manomissione di programmi e di elaboratori; accesso altrui non autorizzato; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	M	Protezione dei locali mediante serratura con distribuzione delle chiavi ai soli autorizzati
	Asportazione e furto di strumenti contenenti dati	Dispersione e perdita di dati, di programmi e di elaboratori;	MB	Protezione dei locali e dei siti di ubicazione degli elaboratori e dei supporti di

		accesso altrui non autorizzato		memorizzazione mediante serratura con distribuzione delle chiavi ai soli autorizzati
	Eventi distruttivi, naturali o artificiali, dolosi, accidentali o dovuti ad incuria	Perdita di dati, dei programmi e degli elaboratori	M	Attività di prevenzione, controllo, assistenza e manutenzione periodica, vigilanza sul rispetto delle istruzioni impartite, formazione e flusso continuo di informazione
	Guasto ai sistemi complementari (impianto elettrico, etc.)	Perdita o alterazione, anche irreversibile, di dati, nonché manomissione dei programmi e degli elaboratori; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	A	Attività di controllo, assistenza e manutenzione periodica backup periodici gruppo di continuità posizionamento personal computer
	Errori umani nella gestione della sicurezza fisica	Perdita o alterazione, anche irreversibile, di dati, nonché manomissione dei programmi e degli elaboratori; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	M	Vigilanza sul rispetto delle istruzioni impartite, formazione e flusso continuo di informazione

5. PROTEZIONE DELLE AREE E DEI LOCALI

Al fine di garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali rilevanti ai fini della loro custodia ed accessibilità, sono state adottate le seguenti misure:

Le aree contenenti dati in supporto cartaceo (mobili ed armadi contenenti documenti) sono ubicate in modo tale che ciascun addetto possa rilevare a vista il tentativo di accesso da parte di persone estranee e, di conseguenza, impedirne l'accesso a persone non autorizzate.

L'ubicazione di stampanti ed apparecchio telefax tradizionale non consente ad estranei di leggere od asportare eventualmente documenti non ancora prelevati dal personale.

Il personale amministrativo, incaricato del trattamento, ha ricevuto le opportune istruzioni per la tutela e la protezione dei dati in formato cartaceo e dei dispositivi informatici attraverso i quali avviene il trattamento dei dati personali.

L'accesso ai locali in cui avviene il trattamento e la custodia di dati personali è vigilato dai Collaboratori Scolastici cui è assegnato il compito di impedire l'intrusione da parte di persone non autorizzate e di identificare e quindi verificare l'autorizzazione all'accesso ai locali dei soggetti ammessi dopo l'orario di chiusura degli uffici.

L'accesso ai locali in cui avviene il trattamento e la custodia di dati personali è vigilato dai Collaboratori Scolastici cui è assegnato il compito di impedire l'intrusione da parte di persone non autorizzate e di

identificare e quindi verificare l'autorizzazione all'accesso ai locali dei soggetti ammessi dopo l'orario di chiusura degli uffici.
Installazione di antivirus sul server e sui pc client al fine di impedire ingressi di pirati o intercettazioni sulla rete informatica di questa istituzione scolastica con la configurazione di password e impostazione di tutte le misure di sicurezza necessarie.
Smaltimento documenti cartacei della segreteria, mediante distruggi documenti

L'Istituzione Scolastica è dotata di impianto elettrico a norma e di appositi estintori.

TRATTAMENTI SENZA AUSILIO DI STRUMENTI ELETTRONICI
Relativamente ai supporti cartacei, i criteri di protezione dei dati debbono essere ricercati nei seguenti:

- qualsiasi documento presentato alla scuola va inserito, quando personale, in apposite cartelline non trasparenti;
- qualsiasi documento che l'istituzione scolastica consegni agli utenti va inserito, quando riservato o contenente documentazione sensibile, in apposite buste o cartelline non trasparenti.
- Le eventuali rubriche telefoniche in utilizzo su supporto cartaceo sono richiuse dopo la consultazione ed il primo foglio delle rubriche stesse, leggibile dall'esterno, non contiene alcun dato (praticamente il primo foglio funge da copertina).
- Tutti i documenti cartacei sono custoditi in idonei armadi posti in locali vigilati
- La scuola è dotata di distruggi documenti

TRATTAMENTI CON STRUMENTI ELETTRONICI
In primo luogo occorre osservare che i computer risultano tutti sollevati da terra, in modo da evitare eventuali danneggiamenti e perdite di dati dovute ad allagamenti.
In secondo luogo si evidenzia che il server è collegato a un gruppo di continuità che consente di prevenire la perdita di dati derivanti da sbalzi di tensione o da interruzione di corrente elettrica. Non appena si dovesse verificare la mancanza di energia elettrica si raccomanda di procedere alla rapida chiusura di qualunque sessione in corso, al salvataggio dei dati sul disco rigido e all'avvio della procedura di spegnimento del server. Ulteriori garanzie sulla protezione delle basi dati sul server sono offerte dalla presenza di dischi rigidi che permette il recupero dei dati anche in presenza di un guasto su uno dei dischi. Nel caso in cui dovesse intervenire il guasto di uno dei dischi del server il responsabile del trattamento dovrà dare immediata comunicazione del fatto all'Amministratore del sistema informatico della rete di segreteria che dovrà procedere all'immediata duplicazione degli archivi del disco e alle operazioni necessarie al ripristino o alla sostituzione del disco difettoso.
Gli incaricati del trattamento hanno ricevuto adeguate istruzioni in merito al trattamento dei dati con lo strumento informatico anche in relazione ai possibili rischi alla integrità ed alla riservatezza dei dati trattati

SISTEMA DI AUTENTICAZIONE ED AUTORIZZAZIONE
Sistema di autenticazione informatica

1. Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.
2. Le credenziali di autenticazione consistono in un codice per l´identificazione dell´incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell´incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell´incaricato, eventualmente associata a un codice identificativo o a una parola chiave.
3. Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l´autenticazione.
4. Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ad uso esclusivo.

5. La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all´incaricato stesso ed è modificata da quest´ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.
6. Il codice per l´identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.
7. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
8. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all´incaricato l´accesso ai dati personali.
9. Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.
10. Quando l´accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l´autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il Titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell´incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l´incaricato dell´intervento effettuato.
11. Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.

Il trattamento di dati personali con strumenti informatici è limitato al personale incaricato al trattamento dotato di un codice per l'identificazione dell'incaricato associato ad una parola chiave riservata conosciuta solo dal medesimo.

Per quanto riguarda il sistema di autorizzazione, a ciascun incaricato del trattamento sono dati i poteri di inserimento, accesso, modifica e cancellazione sui dati relativi a tutte le aree indipendentemente dalla struttura organizzativa cui sono assegnati. Tale scelta si è resa necessaria per garantire la continuità dell'attività amministrativa della segreteria consentendo la sostituzione del personale assente. Eventuali limitazioni all'accesso a determinati dati verranno all'occorrenza determinate modificando i permessi relativi alle password assegnate a ciascun incaricato.

Le credenziali di accesso rilasciate al personale docente permettono l'accesso all'applicazione registro elettronico e dei servizi di segreteria digitale eventualmente attivati ma non ai dati trattati dal personale amministrativo per lo svolgimento della propria attività.

6. DESCRIZIONE DEI CRITERI E DELLE MODALITÀ PER IL RIPRISTINO DELLA DISPONIBILITÀ DEI DATI IN SEGUITO A DISTRUZIONE O DANNEGGIAMENTO

Al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita, è stata definita una procedura di periodica esecuzione di copie di sicurezza dei dati trattati.

In caso di distruzione o danneggiamento dei dati oggetto del trattamento, il soggetto designato delle copie di sicurezza delle banche dati, di concerto con il RESPONSABILE della gestione e manutenzione degli strumenti elettronici, provvederà a ripristinare i dati mediante utilizzo delle copie di backup.

Il soggetto designato può anche prevedere l'utilizzo di altri strumenti in suo possesso (supporti cartacei, e-mail, ...) per ricostruire nel modo più fedele possibile i dati distrutti o danneggiati, sia quelli trattati con l'ausilio di strumenti elettronici che quelli trattati con altri tipi di strumenti. In caso di distruzione o danneggiamento degli strumenti utilizzati per l'accesso ai dati, il Responsabile della gestione e manutenzione degli elaboratori elettronici provvederà tempestivamente al ripristino del normale stato di utilizzo dei suddetti strumenti o alla loro sostituzione.

La procedura di ripristino o di accesso ai dati avverrà comunque in tempi compatibili con i diritti degli interessati in conformità a quanto previsto dall'art. 32 del GDPR.

7. PROGRAMMA DEGLI INTERVENTI FORMATIVI DEGLI INCARICATI DEL TRATTAMENTO E FORMAZIONE DEL PERSONALE

Al Titolare spetta il compito di provvedere all'opportuna formazione di tutti i soggetti designati al trattamento dei dati al fine di:

- garantire il massimo rispetto delle procedure elencate nel presente Documento;
- rendere edotto il personale sui rischi che incombono sui dati e le modalità su come prevenire i danni;
- informare il personale sulle responsabilità che ne derivano.

Il Titolare valuterà opportunamente il livello di preparazione dei singoli addetti in merito alle procedure (informatiche e non) utilizzate per il trattamento e la custodia dei dati; eventuali lacune saranno colmate con appositi interventi formativi volti a rendere i soggetti interessati idonei a svolgere gli incarichi loro assegnati. Il Titolare, con cadenza almeno annuale, provvederà a verificare le esigenze di formazione del personale in base all'esperienza acquisita, al progresso tecnologico o al cambiamento di mansioni.
Tutto il personale incaricato del trattamento dati personali ha seguito il corso, della durata di 9, erogato in modalità e-learning, tramite piattaforma telematica del Ministero Learning@MIUR, avente per oggetto "GDPR – General Data Protection Regulation", rivolto al Personale Amministrativo degli Uffici centrali e periferici del MIUR, finalizzato a guidare il predetto personale in un percorso di adeguamento alla nuova disciplina del GDPR e ai principali cambiamenti in tema di trattamento dei dati personali.
Questa Istituzione Scolastica aderirà alle iniziative formative organizzate dagli uffici centrali e periferici del MIUR, riservandosi comunque di agire in via suppletiva, qualora, per ragioni organizzative od economiche, non sia possibile far partecipare il proprio personale alle attività di formazione necessarie per adempiere alle prescrizioni ordinamentali.

8. CRITERI PREVISTI PER GARANTIRE IL RISPETTO DELLE MISURE MINIME PER I TRATTAMENTI DI DATI PERSONALI AFFIDATI ALL'ESTERNO DELLA STRUTTURA.

L'Istituzione Scolastica, opera il trattamento di dati personali esclusivamente all'interno dell'istituto medesimo e non si avvale di strutture esterne.

ALLEGATI

Sono allegati al presente documento di cui formano parte integrante:

1. registro dei Trattamenti in formato Excel
2. modelli di nomina dei singoli preposti al trattamento dei dati personali, **ai sensi dell'art. 29 del regolamento UE 2016/679**, deputati ad operare sotto la diretta autorità del Titolare del trattamento con allegato "linee guida in materia di sicurezza":

Il Dirigente Scolastico
Prof.ssa Sara BANDINI

Firma autografa, sostituita a mezzo stampa ai sensi dell'art. 3, comma 2 del D.Lgs. 39/1993