

**Documento di valutazione impatto
sulla protezione dei dati personali
D.P.I.A.**

Redatto in base alle indicazioni del Garante Privacy

DATA DI DECORRENZA	COGNOME DIRIGENTE SCOL.	FIRMA D.S.	FIRMA D.P.O.
01/09/2019	MONTICONE		Firmato digitalmente da: Enrico Franco Data: 14/10/2019 11:09:05
01/09/2021	FRESTA AMALIA CR		

DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI PERSONALI

Si redige il seguente documento di valutazione impatto sulla sicurezza dei dati personali che vengono trattati in Istituto, in cui sono individuati

- elenco dei trattamenti (Registro dei Trattamenti)
- misure di sicurezza
- struttura organizzativa per la sicurezza dei dati personali
- misure fisiche e logiche poste a tutela del trattamento dei dati

TITOLARE DEL TRATTAMENTO (Timbro lineare)

Denominazione:	 <p>ISTITUTO COMPRENSIVO SANREMO CENTRO LEVANTE 18038 Sanremo (IM) - Via Volta, 101 C.F. 90083320086 Tel. 0184.50.61.30 @mic813007@istruzione.it imic813007@pec.istruzione.it</p>
Sede del trattamento:	
Codice fiscale o Partita Iva:	
Recapito telefonico :	
Indirizzo e-mail :	
Indirizzo PEC :	

RESPONSABILE DELLA PROTEZIONE DEI DATI (DPO-RPD se richiesto)

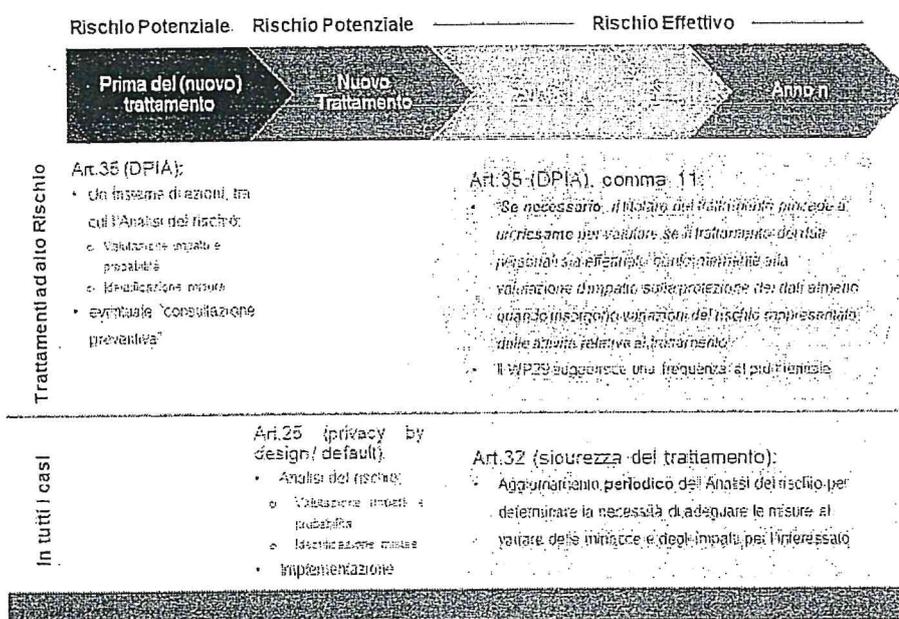
COGNOME E NOME:	FRANCO ENRICO
INDIRIZZO	VIA STUPINIGI N°65 - NICHELINO (TO)
Codice fiscale o Partita Iva:	C.F. FRNNRC60M25L219D - P.I. 09301030012
Recapito telefonico :	340.6083531 / 011.3747246
Indirizzo e-mail :	EFRANCO@FERS-TO.IT
Indirizzo PEC :	EFRANCO@PEC.IT

ELENCO DEI TRATTAMENTI DI DATI PERSONALI (Registro dei trattamenti)

Le operazioni di trattamento effettuate nell'ambito dell'Istituto consistono essenzialmente:

- acquisizione e reperimento dei dati direttamente dalla persona interessata, presso terzi ovvero indirettamente;
- registrazione dei dati, cioè il loro inserimento in supporti informatici o cartacei;
- l'elaborazione;
- la modificazione dei dati registrati, in relazione a variazioni o nuove acquisizioni;
- la conservazione dei dati per tutto il tempo necessario agli scopi per i quali sono stati raccolti o successivamente trattati;
- la cancellazione o la distruzione dei dati, quando sono terminati gli scopi per cui sono stati inizialmente raccolti oppure trascorso il tempo stabilito per quel trattamento.

Attualmente, l'Istituto è titolare dei trattamenti di dati personali riportati nel REGISTRO DEI TRATTAMENTI ed effettua "Trattamenti non occasionali di dati relativi a soggetti vulnerabili" dovendo gestire i dati relativi ai minori



In caso di nuovi trattamenti bisogna procedere con la valutazione preventiva dei flussi e dei punti critici nel trattamento e riportare il nuovo trattamento nel REGISTRO DEI TRATTAMENTI

Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente.

In caso di trattamento di dati personali di particolare rilevanza è almeno semestrale ed i dati vengono digitalmente crittografati.

DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITÀ

Nella tabella allegata al presente documento vengono riportate le strutture presso cui vengono effettuati i trattamenti:

RESPONSABILI DEL TRATTAMENTO E D.P.O./R.P.D. (Se nominati)

Il titolare del trattamento, individua i responsabili del trattamento i quali avranno il compito di controllare sul corretto comportamento del personale dell'Istituto e di affiancare il titolare del trattamento o sostituirlo in caso di temporanea assenza.

A ciascun responsabile, incluso il DPO/RPD, nominato in base alle proprie competenze in materia di gestione dei dati, viene consegnata una specifica lettera di incarico individuale o nomina, nella quale sono fornite precise istruzioni sulle modalità di effettuazione del trattamento e sulle misure di sicurezza da osservare.

INCARICATI o ADDETTI AL TRATTAMENTO

I responsabili del trattamento, hanno individuato gli incaricati / addetti al trattamento a ciascuno dei quali viene consegnata una specifica lettera di incarico individuale, nella quale sono fornite precise istruzioni sulle modalità di effettuazione del trattamento e sulle misure di sicurezza da osservare.

SISTEMA DI AUTENTICAZIONE INFORMATICA

*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 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**.*

*In caso di **videosorveglianza** i dati raccolti dovranno essere mantenuti per un tempo massimo di **48 ore** salvo differenti prescrizioni e non dovranno riprendere attività svolte dai lavoratori se non a fronte di una specifica autorizzazione e comunicazione agli enti preposti.*

ATTUALMENTE NON SONO PRESENTI SISTEMI DI VIDEOSORVEGLIANZA

ANALISI DEI RISCHI CHE INCOMBONO SUI DATI

I rischi ai quali possono essere soggetti i dati trattati dal personale dell'Istituto nell'ambito dell'esercizio della propria normale attività, possono essere: la distruzione o la perdita, anche accidentale; l'accesso non autorizzato; il trattamento non consentito; il trattamento non conforme alle finalità per le quali è avvenuta la raccolta dei dati personali.

si prende in considerazione la lista dei seguenti eventi:

Categoria A : comportamenti degli operatori:

*sottrazione di credenziali di autenticazione
carenza di consapevolezza, disattenzione o incuria
comportamenti sleali o fraudolenti
errore materiale*

Categoria B : eventi relativi agli strumenti:

*azione di virus informatici o di programmi in grado di recare danno (Malware)
spamming o tecniche di sabotaggio elettronico
malfunzionamento, indisponibilità o degrado degli strumenti di elaborazione
accessi esterni non autorizzati
intercettazione di informazioni in rete*

Categoria C : eventi relativi al contesto fisico-ambientale:

*ingressi non autorizzati a locali/aree ad accesso ristretto
sottrazione di strumenti contenenti dati
eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche,
incendi, allagamenti, condizioni ambientali, ecc.), nonché dolosi, accidentali o dovuti ad
incuria guasto a sistemi complementari (impianto elettrico, climatizzazione, ecc.), errori
umani nella gestione della sicurezza fisica*

MISURE IN ESSERE E DA ADOTTARE

Per evitare o ridurre al minimo tutti questi rischi l'Istituto si è dotato di una serie di misure di sicurezza adeguate, di carattere organizzativo, fisico e logico, che riguardano le varie operazioni di trattamento che vengono effettuate ed in particolare la custodia dei dati personali ed il controllo della loro integrità.

***L'allegato documento di analisi dei rischi** raccoglie i rischi individuati e le relative misure adeguate che vengono adottate ed eventuali tempi di attuazione e verifica.*

CRITERI E MODALITÀ DI RIPRISTINO DELLA DISPONIBILITÀ DEI DATI

Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e **non superiori a sette giorni**.

Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con **frequenza almeno settimanale e procedure di ripristino ed emergenza in grado di fronteggiare possibili eventi critici di varia natura**.

PIANIFICAZIONE DEGLI INTERVENTI FORMATIVI

Il presente paragrafo riporta il piano di formazione e le modalità di attuazione:

Descrizione sintetica degli interventi formativi	Classi di incarico o tipologie di incaricati interessati	Tempi previsti
Formazione base per neoassunti	INCARICATI/ADETTI	ENTRO 60 GG DA ASSUNZIONE
Formazione base per nuovi incaricati	INCARICATI/ADETTI	ENTRO 60 GG DAL NUOVO INCARICO
Formazione base per nuovi responsabili	RESPONSABILI	ENTRO 60 GG DAL NUOVO INCARICO
Informazione del personale	INCARICATI/ADETTI	MAIL CON TESTO ALLEGATO

TRATTAMENTI AFFIDATI ALL'ESTERNO, ALL'ESTERO o SU LARGA SCALA

Non sono previsti trattamenti con comunicazione dei dati a paesi terzi all'estero UE o trattamenti biometrici o su LARGA SCALA.

Il trasferimento di dati personali verso l'esterno avviene previo nomina di responsabile al trattamento esterno dell'Ente o della ditta esterna che riceve i dati

PROCEDURE E SISTEMA DI AUDIT PERIODICO

Sono state implementate e reso operative alcune procedure per il rispetto della normativa che vengono allegate, in particolare per la gestione accessi in segreteria, per la progettazione di nuovi trattamenti, per la gestione dei CV e per la modifica e cancellazione dei dati.

Per dimostrare l'applicazione delle procedure e la verifica periodica dei trattamenti effettuati e delle misure in essere sono previsti periodici AUDIT (almeno annuali) effettuati dal DPO con la stesura di apposito verbale o nel caso di AUDIT sul sito WEB di una mail di segnalazione del risultato dell'Audit.

STRUTTURE PRESSO CUI VENGONO EFFETTUATI I TRATTAMENTI:

(DA COMPILARE A MANO)

SEDE	INDIRIZZO	TRATTAMENTI	NOTE
		Cartaceo e Trasferimento Dati	

PLANIMETRIA DEI LOCALI SEDE DEL TRATTAMENTO :

(Allegare planimetria area uffici)

ELENCO DEI RISCHI E MISURE DI PREVENZIONE

CATEG.	RISCHIO	DESCRIZIONE DEL RISCHIO	GRAVITA' STIMATA	MISURA ADOTTATA	TRATTAMENTO INTERESSATO	DATA ATTIVAZIONE	PERIODICITA' CONTROLLI
A	Furto di credenziali di autenticazione (Password e Chiavi armadi)	Accessi non consentiti a dati relativi al personale ed agli allievi	Media (probabilità media, conseguenze medie)	Sensibilizzazione del personale sulla riservatezza delle credenziali	TUTTI	GIA' ATTIVA	SEMESTRALE
A	Carenza di consapevolezza, disattenzione o incuria nella conservazione della documentazione	Perdita di riservatezza di informazioni relative ad allievi, famiglie e dipendenti	Media (probabilità media, conseguenze medie)	Adozione di azioni di controllo per la gestione delle pratiche e informazione di tutto il personale	TUTTI	GIA' ATTIVA	SEMESTRALE
A	Comportamenti sleali o fraudolenti degli addetti	Sottrazione di elenchi ed archivi con perdita di riservatezza di informazioni relative al personale, allievi e fornitori	Media (probabilità media, conseguenze medie)	Adozione di azioni di controllo per la gestione delle pratiche e informazione di tutto il personale	TUTTI	GIA' ATTIVA	SEMESTRALE
A	Errore materiale	Perdita di integrità delle basi di dati e cancellazioni	Bassa	FORMAZIONE E SENSIBILIZZAZIONE+ BACKUP AUTOMATICO	TUTTI	GIA' ATTIVA	SEMESTRALE
B	Azione di virus informatici, di codici malefici o altre azioni fraudolente esterne	Perdita di integrità delle basi di dati e cancellazioni	Media (probabilità media, conseguenze medie)	AGGIORNAMENTO ANTI VIRUS E MALWARE + BACKUP AUTOMATICO	TUTTI	GIA' ATTIVA	SEMESTRALE
B	Spamming, phishing o altre tecniche di sabotaggio	Perdita di integrità delle basi di dati e cancellazioni	Bassa	AGGIORNAMENTO ANTI VIRUS E MALWARE	TUTTI	GIA' ATTIVA	SEMESTRALE
B	Malfunzionamento, indisponibilità o degrado degli strumenti	Perdita di operatività TEMPORANEA	Bassa (probabilità bassa, conseguenze medie)	ASSISTENZA PERIODICA SUI SISTEMI DI BACKUP	TUTTI	GIA' ATTIVA	SEMESTRALE

ELENCO DEI RISCHI E MISURE DI PREVENZIONE

CATEG.	RISCHIO	DESCRIZIONE DEL RISCHIO	GRAVITA' STIMATA	MISURA ADOTTATA	TRATTAMENTO INTERESSATO	DATA ATTIVAZIONE	PERIODICITA' CONTROLLI
B	Accessi esterni non autorizzati alle zone di trattamento dati	Perdita di riservatezza di dati di archivi relativi al personale ai fornitori ed agli allievi	Media (probabilità media, conseguenze medie)	Controlli accurati in ingresso e armadi e uffici chiusi a chiave e distribuzione delle chiavi controllata. DIVIETO DI ACCESSO ALLA SEGRETERIA AL PERSONALE NON AUTORIZZATO	TUTTI	GIA' ATTIVA	SEMESTRALE
B	Intercettazione di informazioni in rete	Perdita di riservatezza di dati di archivi relativi al personale ai fornitori ed agli allievi	Media (probabilità bassa, conseguenze medie)	Controlli periodici sugli accessi alla rete	TUTTI	GIA' ATTIVA	SEMESTRALE
C	Accessi non autorizzati a locali/reparti ad accesso ristretto	Perdita di riservatezza di dati di archivi relativi al personale ai fornitori ed agli allievi	Media (probabilità media, conseguenze medie)	Controlli accurati in ingresso e armadi e uffici chiusi a chiave. DIVIETO DI ACCESSO ALLA SEGRETERIA AL PERSONALE NON AUTORIZZATO	TUTTI	GIA' ATTIVA	SEMESTRALE
C	Asportazione e furto di strumenti contenenti dati	Perdita di riservatezza di dati di archivi relativi al personale ai fornitori ed agli allievi	Bassa (probabilità bassa, conseguenze basse)	Chiusura a chiave dei locali con i server e dei locali di segreteria e presidenza.	TUTTI	GIA' ATTIVA	SEMESTRALE
C	Eventi distruttivi, naturali o artificiali, dolosi, accidentali o dovuti ad incuria	Perdita di operatività TEMPORANEA	Bassa (probabilità molto bassa)	ASSISTENZA PERIODICA SUI SISTEMI DI BACKUP	TUTTI	GIA' ATTIVA	SEMESTRALE
C	Guasto ai sistemi complementari (impianto elettrico, climatizzazione, ...)	Perdita di operatività TEMPORANEA	Bassa (probabilità bassa, conseguenze basse)	Backup dei dati e attesa dei tempi di ripristino	TUTTI	GIA' ATTIVA	SEMESTRALE
C	Errori umani nella gestione della sicurezza fisica: mancata chiusura della sede	Accesso ai dati/agli strumenti di persone non autorizzate	Bassa (probabilità bassa, conseguenze basse)	Controlli accurati in ingresso e armadi e uffici chiusi a chiave.	TUTTI	GIA' ATTIVA	SEMESTRALE

REGISTRO DEI TRATTAMENTI

ID	Indicazione Banca Dati o nome archivio	Struttura/Sede/ Ufficio / Reparto di riferimento	Altre strutture	Tipo di Gestione	Elenco Tipi Trattamenti eseguiti	Finalità	Responsabile Addebi	Strumenti utilizzati per trattamento
	Tempi di conservazione			Natura Dati Trattati		Consenso		Trasferimenti o dati
CURRICULA 1-7 52-53-54-55-57	CURRICULA	SEDE	NO	<input type="checkbox"/> Elettronica <input checked="" type="checkbox"/> Mista <input type="checkbox"/> Cartacea <input checked="" type="checkbox"/> Personal <input checked="" type="checkbox"/> Sensibili <input type="checkbox"/> Giudiziari	<input checked="" type="checkbox"/> Raccolta <input checked="" type="checkbox"/> Consultazione <input checked="" type="checkbox"/> Archiviazione <input type="checkbox"/> Elaborazione <input type="checkbox"/> Aggiornamento <input checked="" type="checkbox"/> Selezione	1.02.01 1.02.05 1.02.05	INTERNI CON APPOSITA PROCEDURA	MISTI <input type="checkbox"/> Esterno <input type="checkbox"/> Estero
5	2 ANNI (salvo protocollo)			<input type="checkbox"/> Elettronica <input type="checkbox"/> Mista <input type="checkbox"/> Cartacea <input type="checkbox"/> Personal <input type="checkbox"/> Sensibili <input type="checkbox"/> Giudiziari	<input type="checkbox"/> Raccolta <input type="checkbox"/> Consultazione <input type="checkbox"/> Archiviazione <input type="checkbox"/> Elaborazione <input type="checkbox"/> Aggiornamento <input type="checkbox"/> Selezione			<input type="checkbox"/> Esterno <input type="checkbox"/> Estero
6				<input type="checkbox"/> Elettronica <input type="checkbox"/> Mista <input type="checkbox"/> Cartacea <input type="checkbox"/> Personal <input type="checkbox"/> Sensibili <input type="checkbox"/> Giudiziari	<input type="checkbox"/> Raccolta <input type="checkbox"/> Consultazione <input type="checkbox"/> Archiviazione <input type="checkbox"/> Elaborazione <input type="checkbox"/> Aggiornamento <input type="checkbox"/> Selezione			<input type="checkbox"/> Esterno <input type="checkbox"/> Estero
7				<input type="checkbox"/> Elettronica <input type="checkbox"/> Mista <input type="checkbox"/> Cartacea <input type="checkbox"/> Personal <input type="checkbox"/> Sensibili <input type="checkbox"/> Giudiziari	<input type="checkbox"/> Raccolta <input type="checkbox"/> Consultazione <input type="checkbox"/> Archiviazione <input type="checkbox"/> Elaborazione <input type="checkbox"/> Aggiornamento <input type="checkbox"/> Selezione			<input type="checkbox"/> Esterno <input type="checkbox"/> Estero
8				<input type="checkbox"/> Elettronica <input type="checkbox"/> Mista <input type="checkbox"/> Cartacea <input type="checkbox"/> Personal <input type="checkbox"/> Sensibili <input type="checkbox"/> Giudiziari	<input type="checkbox"/> Raccolta <input type="checkbox"/> Consultazione <input type="checkbox"/> Archiviazione <input type="checkbox"/> Elaborazione <input type="checkbox"/> Aggiornamento <input type="checkbox"/> Selezione			<input type="checkbox"/> Esterno <input type="checkbox"/> Estero

ALLEGATO A

REGISTRO DEI TRATTAMENTI

Tipo di Banca Dati	ID	Indicazione Banca Dati o nome archivio	Struttura/Sede/ Ufficio /Reparto di riferimento	Altre strutture	Tipo di Gestione Trattati	Elenco Tipi Trattamenti eseguiti	Finalità	Responsabile Addetti	Strumenti utilizzati per trattamento
PERSONALE DOCENTE E NON DOCENTE 6-7 51-52-53-54-55 57	1	LAVORATORI Tempi di conservazione	SEDE/SUCCURS.	SI	Natura Dati Trattati <input type="checkbox"/> Elettronica <input checked="" type="checkbox"/> Mista <input type="checkbox"/> Cartacea	<input checked="" type="checkbox"/> Raccolta <input checked="" type="checkbox"/> Consultazione <input checked="" type="checkbox"/> Archiviazione <input checked="" type="checkbox"/> Elaborazione <input checked="" type="checkbox"/> Aggiornamento <input checked="" type="checkbox"/> Selezione	Consenso 1.01-1.02-1.03 1.04-1.05 1.02.01 2.04	INTERNI ED ESTERNI	MISTI <input checked="" type="checkbox"/> Esterno <input type="checkbox"/> Estero
DATI CONTABILI 51-52-53-54-55- 56-58	2	DATI CONTABILI 10 ANNI	SEDE	NO	<input type="checkbox"/> Elettronica <input checked="" type="checkbox"/> Mista <input type="checkbox"/> Cartacea <input checked="" type="checkbox"/> personali <input checked="" type="checkbox"/> Sensibili <input type="checkbox"/> Giudiziari	<input checked="" type="checkbox"/> Raccolta <input checked="" type="checkbox"/> Consultazione <input checked="" type="checkbox"/> Archiviazione <input checked="" type="checkbox"/> Elaborazione <input checked="" type="checkbox"/> Aggiornamento <input checked="" type="checkbox"/> Selezione	1.03-1.07-1.08 -1.09-1.10	INTERNI ED ESTERNI	MISTI <input checked="" type="checkbox"/> Esterno <input type="checkbox"/> Estero
ALLIEVI e FAMIGLIE 1-7 51-52-53-54-55- 56-57-59-60	3	ALLIEVI e FAMIGLIE 10 ANNI	SEDE/SUCCURS.	SI	<input type="checkbox"/> Elettronica <input checked="" type="checkbox"/> Mista <input type="checkbox"/> Cartacea <input checked="" type="checkbox"/> personali <input checked="" type="checkbox"/> Sensibili <input checked="" type="checkbox"/> Giudiziari	<input checked="" type="checkbox"/> Raccolta <input checked="" type="checkbox"/> Consultazione <input checked="" type="checkbox"/> Archiviazione <input checked="" type="checkbox"/> Elaborazione <input checked="" type="checkbox"/> Aggiornamento <input checked="" type="checkbox"/> Selezione	1.03-1.05-2.04- 5.01-7.06-7.08 7.09-7.10-4.06 -3.06	INTERNI ED ESTERNI	MISTI <input checked="" type="checkbox"/> Esterno <input checked="" type="checkbox"/> Estero
FORNITORI e CONSULENTI 51-52-53-55-56- 57	4	FORNITORI 10 ANNI	SEDE	NO	<input type="checkbox"/> Elettronica <input checked="" type="checkbox"/> Mista <input type="checkbox"/> Cartacea <input checked="" type="checkbox"/> personali <input checked="" type="checkbox"/> Sensibili <input type="checkbox"/> Giudiziari	<input checked="" type="checkbox"/> Raccolta <input checked="" type="checkbox"/> Consultazione <input checked="" type="checkbox"/> Archiviazione <input checked="" type="checkbox"/> Elaborazione <input checked="" type="checkbox"/> Aggiornamento <input checked="" type="checkbox"/> Selezione	1.03-1.09-1.10	INTERNI ED ESTERNI	MISTI <input checked="" type="checkbox"/> Esterno <input type="checkbox"/> Estero

Firmato digitalmente da: Enrico Franco
Data: 14/10/2019 11:30:48

FIRMA R.P.D. / D.P.O. E DATA :

REGISTRO TRATTAMENTI

 Titolare del trattamento	
Nome	
Indirizzo	ISTITUTO COMPRENSIVO SARACINO CENTROLEVANTE
Nr. di telefono	15038 Saracino (RM) - Via Volta, 101 C.F. 90089320086 Tel. 0104-507611-50
Indirizzo e-mail	imic813007@istruzione.it imic813007@pec.istruzione.it
Indirizzo PEC	

 Responsabile per la protezione dei Dati Personali (RPD/DPO)	
Nome	FRANCO ENRICO
Indirizzo	VIA STUPINIGI 65 - NICHELINO (TO)
Nr. di telefono	011-3747246
Indirizzo e-mail	<u>EFRANCO@FERS-TO.IT</u>
Indirizzo PEC	<u>EFRANCO@PEC.IT</u>