Registro TS	**TRATTAMENTO DATI CONSEGUENTE ALL'APPLICAZIONE DELLE MISURE DI CONTENIMENTO DELLA DIFFUSIONE DEL VIRUS SARS-CoV-2**

Descrizione sommaria dell'attività di trattamento	Il trattamento dei dati personali necessari, pertinenti e non eccedenti, avviene allo scopo ultimo di prevenire e contenere il contagio da SARS-CoV-2, in applicazione di un obbligo legale a cui il Titolare del trattamento è sottoposto nonché di eseguire un compito di interesse pubblico ai sensi dell'Art. 6, paragrafo 1 lettera c) ed e) del Regolamento UE 2016/679. Il trattamento inoltre è necessario per motivi di interesse pubblico rilevante come previsto dall'Art. 9, paragrafo 2, lettera g) del medesimo Regolamento UE. Ai sensi dell'Art. 9-ter del D.L. 52/2021 convertito con modificazioni dalla L. 87/2021, introdotto dall'Art. 1 comma 6 del D.L. 111/2021 nonché dal D.P.C.M. 17/06/2021 ss.mm.ii., a far data dal 01/09/2021 e fino al termine dello stato di emergenza, il Datore di Lavoro o un suo delegato richiede, a chiunque acceda ai locali dell'Istituto (ad eccezione degli studenti), l'esibizione del Certificato Verde (green-pass), consentendo l'accesso esclusivamente a chi, in seguito alla lettura del codice a barre bidimensionale (IR Code) mediante l'applicazione "VerificaC19", risulta possedere i requisiti di accesso (Codice VERDE o BLU). Dal 13/09/2021 è stata implementata una nuova funzionalità di verifica automatizzata tramite il Sistema Informativo del Ministero dell'Istruzione SIDI, che interagisce con la Piattaforma nazionale DGC (Digital Green Certificate) del Ministero della Salute, con la finalità di consentire ai Dirigenti Scolastici o loro delegati, il possesso delle certificazioni verdi digitali COVID-19 in corso di validità del personale docente e A.T.A. delle sole scuole statali per consentire agli stessi l'accesso giornaliero nella sede ove prestano servizio. Vigente dal 05/02/2022 l'art. 6 comma 5 del D.L. 05 del 04 Febbraio 2022 consente alle istituzioni scolastiche il controllo della condizione sanitaria degli allievi che consente la didattica in presenza, mediante l'applicazione mobile per la verifica delle certificazioni verdi (Green Pass).	
Finalità del trattamento	ADEMPIMENTI VOLTI ALL'APPLICAZIONE DELLE NORME EMERGENZIALI DI CONTENIMENTO DELLA PANDEMIA ADEMPIMENTI VOLTI ALLA MISURAZIONE DELLA TEMPERATURA CORPOREA DI LAVORATORI, UTENTI E VISITATORI AL FINE DELL'IMPEDIMENTO DI ACCESSO AI SOGGETTI CON TEMPERATURA SUPERIORE AI 37,5°C. ADEMPIMENTI VOLTI AL TRACCIAMENTO DEGLI ACCESSI AI LOCALI DELL'ISTITUTO PER RICOSTRUIRE I CONTATTI ADEMPIMENTI VOLTI AL CONTROLLO DELLA CERTIFICAZIONE VERDE (c.d. GREEN-PASS) E DELLE CERTIFICAZIONI MEDICHE DI NON VACCINABILITA' ADEMPIMENTI VOLTI AL CONTROLLO DELLE CONDIZIONI SANITARIE CHE PERMETTONO AGLI ALLIEVI LA FRUIZIONE DELLA DIDATTICA IN PRESENZA	
Fonte dei dati	**Raccolti direttamente presso gli interessati**	
	LA TOTALITA' DEI DATI E' RACCOLTA DIRETTAMENTE PRESSO GLI INTERESSATI	
	Raccolti presso terzi	
	AZIENDA SANITARIA CON RIFERIMENTO ALL'EMERGENZA SANITARIA IN CORSO MINISTERO DELL'ISTRUZIONE TRAMITE LA PIATTAFORMA SIDI INTERCONNESSA CON LA PIATTAFORMA NAZIONALE DGC (DIGITAL GREEN CERTIFICATE) DEL MINISTERO DELLA SALUTE (SOLO SCUOLE STATALI)	
Base giuridica	**Dati comuni (art. 6 GDPR)**	
	NORMATIVA EMERGENZIALE VIGENTE	
	Dati particolari (art. 9 GDPR)	
	NORMATIVA EMERGENZIALE VIGENTE ART. 9-TER DEL D.L. 52/2021 CONVERTITO CON MODIFICAZIONI DALLA L. 87/2021, INTRODOTTO DALL'ART. 1 COMMA 6 DEL D.L. 111/2021 NONCHÉ DAL D.P.C.M. 17/06/2021 SS.MM.II.	
Natura dei dati oggetto di trattamento	**Comuni**	**Termine trattamento**
	DATI ANAGRAFICI STATO DELLA CERTIFICAZIONE VERDE	14 GIORNI LO STATO DELLA CERTIFICAZIONE VERDE NON VIENE REGISTRATO NEL CASO IN CUI LO STESSO SIA VERDE O BLU MENTRE VIENE REGISTRATO LO STATO "ROSSO" DEL PERSONALE SCOLASTICO E TENUTO AGLI ATTI NEL FASCICOLO PERSONALE DEL DIPENDENTE A FINI DIMOSTRATIVI VISTE LE CONSEGUENZE SANZIONATORIE ED AMMINISTRATIVE CORRELATE LO STATO DELLA CERTIFICAZIONE VERDE RELATIVA AGLI ALLIEVI NON VIENE REGISTRATA
	Particolari	**Termine trattamento**
	DATI INERENTI ALLO STATO DI SALUTE (POSITIVITA', NEGATIVIZZAZIONE ETC.)	FINO ALLA FINE DELLO STATO DI EMERGENZA
	Giudiziari	**Termine trattamento**
	NESSUNO	NESSUNO
Modalità di trattamento dati	I DATI VENGONO TRATTATI IN MODALITA' MISTA, SIA IN FORMATO CARTACEO CHE ELETTRONICO	
Categorie di interessati	DIPENDENTI A TEMPO DETERMINATO E INDETERMINATO, DOCENTI E APPARTENENTI AL PERSONALE A.T.A. ALLIEVI DELL'ISTITUTO E SOGGETTI ESERCENTI LA POTESTA' SU DI ESSI VISITATORI DELL'ISTITUTO CHE ACCEDONO AI LOCALI FORNITORI CHE ACCEDONO AI LOCALI	
	Interni	**Trattamenti eseguiti**

Autorizzati al trattamento	PERSONALE DELLO STAFF DEL DIRIGENTE SCOLASTICO DIRETTORE DEI SERVIZI GENERALI E AMMINISTRATIVI REFERENTI COVID NOMINATI ED AUTORIZZATI INCARICATI DELLA MISURAZIONE DELLA TEMPERATURA CORPOREA AUTORIZZATI DELEGATI AL CONTROLLO DELLA CERTIFICAZIONE VERDE TRAMITE APP "VERIFICAC19" DELEGATI AL CONTROLLO DELLO STATO DELLA CERTIFICAZIONE VERDE TRAMITE IL PORTALE SIDI DEL MINISTERO DELL'ISTRUZIONE INTERCONNESSO CON LA PIATTAFORMA NAZIONALE DGC (DIGITAL GREEN CERTIFICATE) DEL MINISTERO DELLA SALUTE (SOLO SCUOLE STATALI)	RACCOLTA REGISTRAZIONE ORGANIZZAZIONE STRUTTURAZIONE CONSERVAZIONE CONSULTAZIONE ELABORAZIONE SELEZIONE ESTRAZIONE RAFFRONTO UTILIZZO INTERCONNESSIONE BLOCCO COMUNICAZIONE DIFFUSIONE CANCELLAZIONE DISTRUZIONE
	Esterni (Responsabili del Trattamento)	**Trattamenti eseguiti**
	NESSUNO	NESSUNO
Strutture entro le quali avviene il trattamento dati	**Dati in formato cartaceo**	**Archiviazione storica dati cartacei**
	UFFICIO DEL DIRIGENTE SCOLASTICO E SUOI VICE	UFFICIO DEL DIRIGENTE SCOLASTICO E SUOI VICE
	Dati in formato elettronico	**Archiviazione storica dati elettronici**
	SERVER DI SEGRETERIA	UNITA' DI BACK UP DEL SERVER
	Software impiegati per il trattamento informatico dei dati in formato elettronico	
	MICROSOFT OFFICE	REGISTRO ELETTRONICO

Possibili destinatari di attività di comunicazione	**Comunicazioni istituzionali**	**Extra UE**	**Comunicazioni su base volontaria**	**Extra UE**
	AMMINISTRAZIONE SCOLASTICA I.N.A.I.L. AZIENDA SANITARIA LOCALE / A.T.S. R.S.P.P. MEDICO COMPETENTE	NO	COMPAGNIE DI ASSICURAZIONE	NO
Informativa	VIENE FORNITA INFORMATIVA SPECIFICA SIA MEDIANTE APPOSIZIONE DI CARTELLONISTICA AL PUNTO IN CUI AVVIENE IL TRATTAMENTO (CONTROLLO TEMPERATURA E CONTROLLO CERTIFICAZIONE VERDE) SIA, NEL CASO DEL CONTROLLO DEL GREEN-PASS, MEDIANTE PUBBLICAZIONE DI INFORMATIVA DETTAGLIATA SUL SITO ISTITUZIONALE			
Profilazione	NON VIENE ATTUATA NESSUNA ATTIVITA' DI PROFILAZIONE			
Frequenza	IL TRATTAMENTO AVVIENE CON FREQUENZA QUOTIDIANA E PER TUTTA LA DURATA DELLO STATO DI EMERGENZA COME DECISO DAL PARLAMENTO ITALIANO			

Valutazione del rischio	**TRATTAMENTO**	**PROBABILITA' (P)**	**CONSEGUENZE (C)**	**LIVELLO DI RISCHIO (R)**
	GENERALE	POCO PROBABILE	GRAVI	**RILEVANTE**
	REGISTRO ELETTRONICO	POCO PROBABILE	GRAVI	**RILEVANTE**

Valutazione della obbligatorietà della DPIA	L'esito della valutazione dei rischi mostra un livello di rischio ELEVATO per i diritti e le libertà delle persone fisiche interessate ?	**NO**
	L'attività comporta procedimenti valutativi, di scoring o di profilazione ?	**NO**
	L'attività comporta la presa di decisioni automatizzate che producono significativi effetti giuridici (ammissioni, assunzioni, concessioni etc.) ?	**NO**
	L'attività comporta il monitoraggio sistematico di persone fisiche (videosorveglianza ad esempio) ?	**NO**
	L'attività comporta il trattamento di dati particolari, giudiziari o di natura estremamente personale (es. opinioni politiche) ?	**SI**
	L'attività comporta il trattamento di dati personali su larga scala ?	**NO**
	L'attività comporta la combinazione o il raffronto di insiemi di dati derivanti da due o più trattamenti svolti per diverse finalità e/o da titolari distinti, secondo modalità che esulano dal contesto iniziale (big data) ?	**NO**
	L'attività comporta il trattamento di dati relativi a soggetti vulnerabili (minori, soggetti con patologie psichiatriche, richiedenti asilo, anziani etc.) ?	**NO**
	L'attività comporta utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative (riconoscimento facciale ad esempio) ?	**NO**
	L'attività comporta trattamenti che, di per sé, potrebbero impedire agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto (es: screening dei clienti di una banca attraverso i dati registrati in una centrale rischi per stabilire la concessione di un finanziamento).	**NO**

SI CONCLUDE LA VALUTAZIONE A FAVORE DELLA NON NECESSITA' DI ESEGUIRE LA DPIA PER QUESTO TRATTAMENTO

AL FINE DEL CONTENIMENTO DEL RISCHIO SONO ADOTTATE LE SEGUENTI MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE:

MISURA DI SICUREZZA	RISCHIO CONTRASTATO	
E' adottata una politica di istituto per la sicurezza e la protezione dei dati ed all'interno dell'Istituto sono definiti i ruoli e le responsabilità di ciascuno anche mediante consegna di lettere di autorizzazione dettagliate	- Eventi naturali ed agenti fisici (terremoti, incendi, allagamenti etc.); - Compromissione delle informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, etc.); - Azioni non autorizzate (errori volontari o involontari, virus, uso non autorizzato di strumentazione, etc.).	
Sono utilizzati software antivirus e firewall	- Compromissione delle informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, etc.); - Azioni non autorizzate (virus, accessi non autorizzati, utilizzo di supporti non autorizzati, uso non autorizzato di strumentazione, etc.).	

Vengono attuati i *back up* con frequenza quotidiana	- Eventi naturali ed agenti fisici (terremoti, incendi, allagamenti etc.); - Problemi tecnici (anomalie e malfunzionamento software, problemi hardware); - Interruzione servizi (sbalzi di tensione, guasti all'impianto, interruzione collegamenti di rete, etc.); - Furto di dati e distruzione volontaria ed involontaria.	
Sono applicate, da parte del soggetto incaricato dell'amministrazione del sistema informatico, procedure di *"disaster recovery"* che garantiscono il ripristino dell'accesso ai dati in tempi ridotti	- Eventi naturali ed agenti fisici (terremoti, incendi, allagamenti etc.); - Problemi tecnici (anomalie e malfunzionamento software, problemi hardware); - Interruzione servizi (sbalzi di tensione, guasti all'impianto, interruzione, collegamenti di rete, etc.); - Azioni di danneggiamento volontario.	
Sono adottati sistemi di cifratura e anonimizzazione dei dati relativi allo stato di salute delle persone	- Azioni non autorizzate (errori volontari o involontari, virus, uso non autorizzato di strumentazione, etc.); - Compromissione delle informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, etc.); - Furto e sottrazione di dati	
Sono registrati da parte del soggetto incaricato dell'amministrazione del sistema informatico, i *"log-file"* al fine di ricostruire gli accessi ai database	- Azioni non autorizzate (errori volontari o involontari, uso non autorizzato di strumentazione, supporti etc.); - Compromissione delle informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, etc.).	
Viene eseguita periodica manutenzione della rete informatica in cui si esegue il trattamento dei dati al fine di controllare periodicamente il funzionamento regolare di antivirus, firewall nonché assicurare l'aggiornamento dei sistemi operativi in uso e di tutti i presidi di sicurezza attiva	- Problemi tecnici (anomalie e malfunzionamento software, problemi hardware).	
I Data Center di cui l'Istituto di serve sono in possesso di certificazione ISO	- Compromissione delle informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, etc.); - Azioni non autorizzate (errori volontari o involontari, virus, uso non autorizzato di strumentazione, etc.); - Problemi tecnici (anomalie e malfunzionamento software, problemi hardware).	
I singoli incaricati vengono formalmente autorizzati al trattamento dei dati ed a ciascuno vengono fornite credenziali personali (nome utente e *password*) per eseguire l'accesso ai sistemi informatici	- Azioni non autorizzate (errori volontari o involontari, protezione da virus e malware in genere, uso non autorizzato di strumentazione, etc.); - Compromissione delle informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, etc.); - Problemi tecnici (anomalie e malfunzionamento software).	
Le credenziali di autenticazione fornite ai singoli incaricati sono disattivate in caso di assenza della persona prolungata per oltre 6 mesi	- Compromissione delle informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica etc. da parte di soggetti non più autorizzati); - Azioni non autorizzate (errori volontari o involontari, uso non autorizzato di strumentazione, etc.).	
Le credenziali di autenticazione fornite ai singoli incaricati sono disattivate o i profili di accesso sono modificati per colui che, a causa di un cambiamento di mansione, perda la possibilità di trattare i dati o se la veda modificata	- Compromissione delle informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica etc. da parte di soggetti non più autorizzati); - Azioni non autorizzate (errori volontari o involontari, virus, uso non autorizzato di strumentazione, etc.).	
I sistemi di autorizzazione prevedono la presenza di diversi profili di autorizzazione, l'individuazione preventiva per incaricato, l'individuazione preventiva per classi omogenee di incaricati, la verifica almeno annuale dei profili	- Azioni non autorizzate (errori volontari o involontari, virus, uso non autorizzato di strumentazione, etc.); - Compromissione delle informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, etc. eseguita da parte dichi non è più autorizzato a trattare i dati).	
Le parole chiave (*password*) fornite sono complesse (lunghe almeno 8 caratteri e formate da lettere e numeri, maiuscole e minuscole) e non sono riferibili a condizioni personali dell'autorizzato. Le password devono essere modificate la primo accesso e devono essere cambiate ogni 3 mesi	- Compromissione delle informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, etc.); - Azioni non autorizzate (errori volontari o involontari, virus, uso non autorizzato di strumentazione, etc.); - Evitare che l'accesso ai dati digitali possa avvenire troppo facilmente.	
Esclusivamente ai singoli incaricati viene concesso l'accesso ai locali (uffici, sale docenti, archivi, CED etc.) ed agli arredi (cassetti, armadi,	- Azioni non autorizzate (errori volontari o involontari, virus, uso non autorizzato di strumentazione, etc.); - Compromissione delle informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, etc.); - Problemi tecnici (anomalie e malfunzionamento software, problemi hardware);	

schedari etc.) in cui devono prestare la loro attività di trattamento	- Evitare che l'accesso ai dati cartacei ed agli elaboratori possa avvenire troppo facilmente.	
I locali in cui avviene il trattamento dati sono dotati di presidi antincendio	- Eventi naturali ed agenti fisici (terremoti, incendi, allagamenti etc.);	
Le prese di alimentazione elettrica a cui sono connessi gli apparati informatici di rete nonché server ed elaboratori forniscono idonee garanzie di stabilità	- Problemi tecnici (anomalie e malfunzionamento software, problemi hardware); - Interruzione servizi (sbalzi di tensione, guasti all'impianto, interruzione collegamenti di rete, etc.).	
I locali in cui avviene il trattamento dati, al termine dell'attività, vengono chiusi a chiave così come cassetti ed armadi contenenti dati personali, le chiavi sono nella disponibilità di soli soggetti autorizzati a detenerle	- Azioni non autorizzate (errori volontari o involontari, virus, uso non autorizzato di strumentazione, etc.); - Compromissione delle informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, etc.); - Problemi tecnici (anomalie e malfunzionamento software, problemi hardware).	
I supporti cartacei contenenti dati personali non più necessari vengono distrutti fisicamente prima della loro eliminazione	- Accesso da parte di soggetti non autorizzati;	
I supporti magnetici (chiavette, dischi removibili etc.) contenenti dati personali non più necessari vengono distrutti fisicamente prima della loro eliminazione	- Accesso da parte di soggetti non autorizzati;	
Ai singoli utenti autorizzati vengono fornite istruzioni per la custodia e l'uso di supporti removibili	- Azioni non autorizzate (errori volontari o involontari, virus, uso non autorizzato di strumentazione, etc.); - Eventi naturali ed agenti fisici (terremoti, incendi, allagamenti etc.); - Perdita, smarrimento, furto.	
E' prevista l'organizzazione periodica di corsi di formazione ed interventi informativi volti a fornire nozioni ed a sensibilizzare il personale autorizzato	- Azioni non autorizzate (errori volontari o involontari, virus, uso non autorizzato di strumentazione, etc.); - Perdita, smarrimento.	
Il personale autorizzato è soggetto alla vigilanza del Titolare del trattamento e degli altri autorizzati con compiti di coordinamento e direttivi	- Azioni non autorizzate (errori volontari o involontari, virus, uso non autorizzato di strumentazione, etc.); - Furti, danneggiamenti volontari; - Uso non autorizzato di supporti personali; - Uso illegale di software.	
Tutte le procedure sono oggetto di riesame almeno annuale in occasione dell'audit periodico eseguito dal D.P.O.	- Azioni non autorizzate (errori volontari o involontari, virus, uso non autorizzato di strumentazione, etc.); - Compromissione delle informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, etc.); - Problemi tecnici (anomalie e malfunzionamento software, problemi hardware); - Verifica della corretta applicazione delle norme regolamentari.	
I dati non sono diffusi o comunicati a terzi al di fuori delle specifiche previsioni normative	- Azioni non autorizzate (errori volontari o involontari, virus, uso non autorizzato di strumentazione, etc.).	
Sono definiti termini di conservazione e le condizioni di impiego e successiva distruzione dei dati personali trattati	- Azioni non autorizzate (errori volontari o involontari, virus, uso non autorizzato di strumentazione, etc.); - Compromissione delle informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, etc.).	
Ancorché non obbligatoria, su questo trattamento viene eseguita la DPIA (Data Protection Impact Assesment)	- Compromissione delle informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, etc.); - Azioni non autorizzate (errori volontari o involontari, virus, uso non autorizzato di strumentazione, etc.).	

Sant'Onofrio
8/2/2022

IL DIRIGENTE SCOLASTICO
Prof.ssa Marzia Arrigoni