Registro Trattamento Dati

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

Istituto Comprensivo Puccini
Viale Donato Giannotti, 41, 50126 Firenze FI

REV.00 di Ottobre 2020

1. NOME E DATI DEL TITOLARE DEL TRATTAMENTO

Titolare del trattamento:
Istituto Comprensivo Puccini Viale D. Giannotti, 41 50126 Firenze (FI)

Legale Rappresentante: Prof. Mattia Venturato

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	✓ 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	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.).
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
FINALITÀ 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, 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.

DEI DATI A TERZI PER IL TRATTAMENTO:	Tutti i dati posseduti dalla scuola vengono trattati esclusivamente presso gli Uffici dell'Istituto e piattaforme di gestione documentale pubbliche e/o 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.
MODALITA' DI CONSERVAZIONE	ARCHIVIO 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. Alcuni dati personali non sensibili possono essere riposti in armadi senza serratura ospitati in locali vigilati e sotto il controllo dei collaboratori scolastici anche dopo l'orario di chiusura degli uffici.
	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. Attraverso 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.

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 del'ert. 4 del Regolamento UE 2016/679, il Titolare è "… la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il Titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri …".
L'art. 4 sopra richiamato individua anche un altro soggetto di rilevante importanza nell'ambito del Trattamento dei dati personali. Si tratta del Responsabile del trattamento e cioè "… la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento …".
Si tratta di un soggetto, distinto dal Titolare, che deve essere in grado di fornire garanzie al fine di assicurare il pieno rispetto delle disposizioni in materia di trattamento dei dati personali, nonché di garantire la tutela dei diritti dell'interessato. Il responsabile del trattamento dovrà avere innanzitutto una competenza qualificata, dovendo garantire una conoscenza specialistica della materia, e l'attuazione delle misure tecniche e organizzative in grado di soddisfare i requisiti stabiliti dal regolamento europeo. Inoltre dovrà garantire una particolare affidabilità, un requisito fondato su aspetti etici e deontologici (ad esempio, l'assenza di condanne penali).
Orbene, considerato che il Regolamento UE non prevede, per il Titolare che si avvale di soggetti interni per il trattamento dei dati personali, alcun obbligo di nomina di un Responsabile del trattamento e che tra il personale interno non vi è alcuno che presenti quella competenza qualificata, il Titolare del trattamento non designa alcun responsabile del trattamento.
Pertanto, incombe sullo stesso Titolare del trattamento l'onere:

- ✓ individuare ed adottare le misure di sicurezza da applicare nell'ambito dell'Istituzione Scolastica, al fine di salvaguardare la riservatezza, l'integrità, la completezza e la disponibilità dei dati trattati;
- ✓ provvedere, mediante atto scritto, all'individuazione singoli preposti, ai sensi dell'art. 29 del regolamento UE 2016/679, deputati ad operare sotto la sua diretta autorità attenendosi alle istruzioni impartite;
- ✓ all'esigenza di verificare che gli obblighi di informativa siano stati assolti correttamente, ovvero che sia stato conseguito il consenso degli interessati;
- ✓ adempiere alle richieste avanzate dal Garante per la protezione dei dati personali ovvero alle autorità investite dei poteri di controllo;
- ✓ osservare e far osservare il divieto di comunicazione e diffusione dei dati personali comunque trattati da parte dell'Istituzione Scolastica;
- ✓ proporre soluzioni organizzative che consentano un ampliamento dei livelli di sicurezza.

Il personale, docente e non docente, (individuato mediante atti allegati al presente Documento), preposto al trattamento **è autorizzato al trattamento** dei dati in possesso dell'Istituzione Scolastica, esclusivamente con riferimento all'espletamento delle funzioni istituzionali ad essi rispettivamente assegnate.
Il personale preposto al trattamento, in particolare, è stato edotto in merito alla circostanza che:

- ✓ il trattamento e la conservazione dei dati deve avvenire esclusivamente in modo lecito e proporzionato alle funzioni istituzionali, nel rispetto della riservatezza;
- ✓ la raccolta, registrazione ed elaborazione dei dati, mediante strumento informatico o cartaceo, deve essere limitata alle finalità istituzionali;
- ✓ la correzione od aggiornamento dei dati posseduti, l'esame della loro pertinenza rispetto alle funzioni, deve essere costante;
- ✓ d) la comunicazione o diffusione dei dati personali deve avvenire esclusivamente a soggetti autorizzati a riceverli legittimamente per le finalità per le quali sono stati raccolti e comunque nel rispetto delle istruzioni ricevute.

L'ambito dei trattamenti autorizzati ai singoli Preposti suscettibile di aggiornamento periodico.
A tutti gli incaricati destinati al trattamento di dati mediante strumento elettronico, sono state conferite credenziali di autenticazioni mediante parola chiave.

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:

SIGLA	LIVELLO DI RISCHIO
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		Gravità stimata	
COMPORTAMENTI DEGLI OPERATORI	Furto di credenziali di autenticazione	→ Accesso altrui non autorizzato	**M**	✓ Vigilanza sul rispetto delle istruzioni impartite ✓ Formazione del personale ✓ Formazione e flusso continuo di informazione
	Carenza di consapevolezza, disattenzione o incuria	→ Dispersione, perdita e accesso altrui non autorizzato	**M**	
	Comportamenti sleali o fraudolenti	→ Dispersione, perdita e accesso altrui non autorizzato	**M**	
	Errore materiale	→ Dispersione, perdita e accesso altrui non autorizzato	**M**	
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 ✓ Assistenza e manutenzione continua degli elaboratori e dei programmi; ricambio periodico
	Spamming o altre tecniche di sabotaggio	→ Perdita o alterazione, anche irreversibile, di dati, di programmi e di elaboratori; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	**EE**	
	Malfunzionamento, indisponibilità o degrado degli	→ Perdita o alterazione, anche irreversibile, di dati, di programmi e di	**MA**	

	strumenti		elaboratori; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	
	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**
	Intercettazione di informazioni in rete	→	Dispersione di dati; accesso altrui non autorizzato	**MA**
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**
	Asportazione e furto di strumenti contenenti dati	→	Dispersione e perdita di dati, di programmi e di elaboratori;	**MB**
	Eventi distruttivi, naturali o artificiali, dolosi, accidentali o	→	Perdita di dati, dei programmi e degli elaboratori	**M**

- ✓ Protezione dei locali mediante serratura con distribuzione delle chiavi ai soli autorizzati
- ✓ Protezione dei locali e dei siti di ubicazione degli elaboratori e dei supporti di
- ✓ memorizzazione mediante serratura con distribuzione delle chiavi ai soli autorizzati
- ✓ Attività di prevenzione, controllo, assistenza e manutenzione periodica, vigilanza sul rispetto delle istruzioni impartite, formazione e flusso continuo di informazione
- ✓ Attività di controllo, assistenza e manutenzione periodica

	dovuti ad incuria			✓ backup periodici ✓ gruppo di continuità ✓ posizionamento personal computer ✓ 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**
	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**

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.
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.
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 L'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 è opportuno che i computer siano sollevati da terra, in modo da evitare eventuali danneggiamenti e perdite di dati dovute ad allagamenti.
In secondo luogo è necessario che il server sia collegato a un gruppo di continuità che consenta di prevenire la perdita di dati derivanti da sbalzi di tensione o da interruzione di corrente elettrica.
Ad ogni modo saranno previsti Backup periodici.
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 ed uso esclusivo dell´incaricato
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 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.
Le copie di sicurezza sono custodite negli uffici della sede centrale.
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 provvederà a verificare le esigenze di formazione del personale in base all'esperienza acquisita, al progresso tecnologico o al cambiamento di mansioni.

Funzione di business/Unità Organizzativa/Dipartimento: Segreteria didattica

Denominazione del trattamento: Gestione Attività educativa, didattica, formativa e di valutazione

Finalità del trattamento	Software, Database, Manutenzione	Categorie di interessati	Categorie di dati personali	Categorie di destinatari a cui i dati sono o possono essere comunicati	Periodo di conservazione dei dati	Articolo 6 (base giuridica su cui si fonda il trattamento)	Articolo 9 (base giuridica per il trattamento di particolari categorie di dati)	Tipologia di trattamento	Fonte dei dati personali (se applicabile)	Denominazione responsabili esterni (se presenti)
erogazione del servizio di istruzione	Axios SIDI	Alunni/famiglie	Dati identificativi della persona: Cognome, Nome, data di nascita, luogo di nascita, codice fiscale, residenza, domicilio, telefono, email, Dati particolari: giudiziari, religione, salute	MIUR, Altre istituzioni scolastiche, AUSL, Enti Locali, Gestori pubblici e privati dei servizi di assistenza, Istituti di assicurazione, INAIL, Aziende, imprese e altri soggetti pubblici o privati, Avvocature dello Stato, Ufficio scolastico provinciale	Termine delle finalità per le quali il dato è stato raccolto	Obbligo legale	obblighi in materia di frequenza obbligatoria	registrazione informatica, comunicazione, estrazione, copia, utilizzo, cancellazione, conservazione.	dell'interessato Comune	Axios SIDI
Gestione servizio mensa	Axios						obblighi in materia di frequenza obbligatoria, interesse sanità pubblica		dell'interessato Comune	Axios
Registrazione presenza, Valutazione - Registro elettronico	Axios SIDI						obblighi in materia di frequenza obbligatoria, interesse sanità pubblica		dell'interessato	Axios SIDI
infortuni	SIDI						obblighi in materia di frequenza, sicurezza luoghi di lavoro		dell'interessato	SIDI
viaggi d'istruzione e visite guidate	=						il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare.		dell'interessato	=

Descrizione generale delle misure di sicurezza adottate (se possibile):

- ✓ Gestione cartacea: presidio punti di stampa
- ✓ Controllo accesso locali amministrativi;
- ✓ Antivirus con controllo rete
- ✓ Procedure di backup e disaster recovery;
- ✓ Nomina per iscritto personale;
- ✓ Armadi chiusi;
- ✓ Nomina per iscritto responsabili esterni;

- ✓ Policy aziendali;
- ✓ Modifica credenziali;
- ✓ Programmazione della formazione del personale
- ✓ Rispetto normative anticendio
- ✓ Presenza presidi antincendio

Modalità di conservazione dei dati:

- ✓ Anaogico
- ✓ Digitale

PLURY Consulting

Funzione di business/Unità Organizzativa/Dipartimento: Segreteria del Personale - Area personale

Denominazione del trattamento: orto di lavoro del personale docente e ATA, gestione contratti (assunzione), Sicurezza sul lavoro, congedi , scioperi e assenze

Finalità del trattamento	Software, Database, Manutenzione	Categorie di interessati	Categorie di dati personali	Categorie di destinatari a cui i dati sono o possono essere comunicati	Periodo di conservazione dei dati	Articolo 6 (base giuridica su cui si fonda il trattamento)	Articolo 9 (base giuridica per il trattamento di particolari categorie di dati)	Tipologia di trattamento	Fonte dei dati personali (se applicabile)	Denominazione responsabili esterni (se presenti)
Amministrazione del personale	Axios SIDI	docenti ATA	Dati relativi alla prestazione lavorativa, dati anagrafici, formazione, dati sanitari	INPS; ragioneria MEF, MIUR, Agenzia delle Entrate, Corte dei Conti, Enti assistenziali, previdenziali e assicurativi, Banca che effettua il servizio di cassa	5 anni	Obbligo legale	Esercizio obblighi in materia di diritto del lavoro	Comunicazione, estrazione, copia, duplicazione, cancellazione, conservazione	raccolta presso interessati e presso terzi	Axios SIDI
avvio collaborazione	Axios SIDI	docenti ATA	Dati relativi alla prestazione lavorativa, dati anagrafici, formazione		Termine delle finalità per le quali il dato è stato raccolto	Obbligo legale	Esercizio obblighi in materia di diritto del lavoro			Axios SIDI
Tutela sicurezza sul lavoro	Axios SIDI	Lavoratori Alunni	Formazione, dati anagrafici, giudizio idoneità	RSPP, Medico Competente, INAIL, Enti, Agenzie Formative, compagnie assicurative.	Termine delle finalità per le quali il dato è stato raccolto	Obbligo legale	Esercizio obblighi in materia di sicurezza sul lavoro			RSPP, Medico Competente,
gestione assenze	Axios SIDI	docenti ATA	Dati relativi alla prestazione lavorativa, dati sanitari	INPS; ragioneria MEF, MIUR, Agenzia delle Entrate, Corte dei Conti, Enti assistenziali, previdenziali e assicurativi, Banca che effettua il servizio di cassa	Termine delle finalità per le quali il dato è stato raccolto	Obbligo legale	Esercizio obblighi in materia di diritto del lavoro			Axios SIDI

Descrizione generale delle misure di sicurezza adottate (se possibile):

- ✓ Gestione cartacea: presidio punti di stampa
- ✓ Controllo accesso locali amministrativi;
- ✓ Antivirus con controllo rete
- ✓ Procedure di backup e disaster recovery;
- ✓ Nomina per iscritto personale;
- ✓ Armadi chiusi;
- ✓ Nomina per iscritto responsabili esterni;
- ✓ Policy aziendali;
- ✓ Modifica credenziali;
- ✓ Programmazione della formazione del personale
- ✓ Rispetto normative anticendio
- ✓ Presenza presidi antincendio

Modalità di conservazione dei dati:

- ✓ Anaogico
- ✓ Digitale

Funzione di business/Unità Organizzativa/Dipartimento: Segreteria Amministrativa contabile										
Denominazione del trattamento: Gestione economico-finanziaria delle risorse assegnate alla scuola, manutenzione edificio, gestione fatturazione,										
Finalità del trattamento	**Software, Database, Manutenzione**	**Categorie di interessati**	**Categorie di dati personali**	**Categorie di destinatari a cui i dati sono o possono essere comunicati**	**Periodo di conservazione dei dati**	**Articolo 6 (base giuridica su cui si fonda il trattamento)**	**Articolo 9 (base giuridica per il trattamento di particolari categorie di dati)**	**Tipologia di trattamento**	**Fonte dei dati personali (se applicabile)**	**Denominazione responsabili esterni (se presenti)**
Contratti, convenzioni, protocolli d'intesa, accordi di programma	Axios, SIDI, Consip, Mepa,	contraente, partecipante alla selezione del contraente, firmatari dell'intesa/accordo FORNITORI	Dati identificativi della persona: Cognome, Nome, data di nascita, luogo di nascita, codice fiscale, residenza, domicilio, telefono, email, PEC. Dati particolari: giudiziari, situazione economico-patrimoniale	DITTE VARIE/BANCA/SIDI/CONSIP/AGENZIA DELLE ENTRATE	Termine delle finalità per le quali il dato è stato raccolto	Obbligo legale D.LGS. 50/2016 Decreto Interministeriale 1 febbraio 2001, n.44	Tracciabilità flussi finanziari	Gestione cartacea: richiesta acquisto o manutenzione; avvisi per procedura diretta; bandi gara; determina; prospetti comparativi; cig; ordine	raccolta presso interessati e presso terzi	Axios, SIDI, Consip, Mepa,
acquisizione di un bene			dati di identificazione finanziaria							
manutenzione edifico/mobili/attrezzature										
Mandati di pagamento				INAIL; Assicurazioni						

Descrizione generale delle misure di sicurezza adottate (se possibile):

- ✓ Gestione cartacea: presidio punti di stampa

- ✓ Controllo accesso locali amministrativi;
- ✓ Antivirus con controllo rete
- ✓ Procedure di backup e disaster recovery;
- ✓ Nomina per iscritto personale;
- ✓ Armadi chiusi;
- ✓ Nomina per iscritto responsabili esterni;
- ✓ Policy aziendali;
- ✓ Modifica credenziali;
- ✓ Programmazione della formazione del personale
- ✓ Rispetto normative anticendio
- ✓ Presenza presidi antincendio

Modalità di conservazione dei dati:

- ✓ Anaogico
- ✓ Digitale

Funzione di business/Unità Organizzativa/Dipartimento: Segreteria Amministrativa contabile										
Denominazione del trattamento: Attività di protocollazione relativa all'acquisizione di atti e documenti e all'inoltro di atti e documenti										
Finalità del trattamento	**Software, Database, Manutenzione**	**Categorie di interessati**	**Categorie di dati personali**	**Categorie di destinatari a cui i dati sono o possono essere comunicati**	**Periodo di conservazione dei dati**	**Articolo 6 (base giuridica su cui si fonda il trattamento)**	**Articolo 9 (base giuridica per il trattamento di particolari categorie di dati)**	**Tipologia di trattamento**	**Fonte dei dati personali (se applicabile)**	**Denominazione responsabili esterni (se presenti)**
acquisizione dati personali contenuti in atti e documenti amministrativi	Axios	studenti, personale ATA, docenti, soggetti esterni	Dati identificativi della persona: Cognome, Nome, data di nascita, luogo di nascita, codice fiscale, residenza, domicilio, telefono, email, PEC. Dati particolari: salute, giudiziari, situazione economico-patrimoniale	USP, USR, MIUR, Altre istituzioni scolastiche, Ordinario Diocesano, Organizzazioni Sindacali, Presidenza del Consiglio, INPDAP, INPS, INAIL, AUSL, Altre Amministrazioni Pubbliche, Corte dei Conti, MEF, Enti assistenziali, previdenziali e assicurativi, Organi preposti alla vigilanza su igiene e sicurezza, Autorità di pubblica Sicurezza, Agenzia delle Entrate, Organi preposti agli accertamenti idoneità impiego, Banca che effettua il servizio di cassa, Ufficio scolastico regionale dello Stato	Termine delle finalità per le quali il dato è stato raccolto	Obbligo legale d.lgs 82/2005	Obbligo legale	Comunicazione, estrazione, copia, duplicazione, cancellazione, conservazione	raccolta presso interessati	Axios,
Descrizione generale delle misure di sicurezza adottate (se possibile): ✓ Gestione cartacea: presidio punti di stampa ✓ Controllo accesso locali amministrativi; ✓ Antivirus con controllo rete										

- ✓ Procedure di backup e disaster recovery;
- ✓ Nomina per iscritto personale;
- ✓ Armadi chiusi;
- ✓ Nomina per iscritto responsabili esterni;
- ✓ Policy aziendali;
- ✓ Modifica credenziali;
- ✓ Programmazione della formazione del personale
- ✓ Rispetto normative anticendio
- ✓ Presenza presidi antincendio

Modalità di conservazione dei dati:

- ✓ Anaogico
- ✓ Digitale

Funzione di business/Unità Organizzativa/Dipartimento: Segreteria Amministrativa contabile

Denominazione del trattamento: Gestione archivio cartaceo storico

Finalità del trattamento	Software, Database, Manutenzione	Categorie di interessati	Categorie di dati personali	Categorie di destinatari a cui i dati sono o possono essere comunicati	Periodo di conservazione dei dati	Articolo 6 (base giuridica su cui si fonda il trattamento)	Articolo 9 (base giuridica per il trattamento di particolari categorie di dati)	Tipologia di trattamento	Fonte dei dati personali (se applicabile)	Denominazione responsabili esterni (se presenti)
archiviazione della documentazione amministrativa e didattica	Axios	alunno, famiglie, docenti, ATA	Dati identificativi della persona: Cognome, Nome, data di nascita, luogo di nascita, codice fiscale, residenza, domicilio, telefono, email, PEC. Dati particolari: salute, giudiziari, situazione economico-patrimoniale, dati relativi allo stato di salute	Altre Amministrazioni Pubbliche sulla base dell'interesse pubblico al trattamento, soggetti privati se previsto da norme di legge o regolamento	Termine delle finalità per le quali il dato è stato raccolto	Obbligo legale	Obbligo legale	Comunicazione, estrazione, copia, duplicazione, cancellazione, conservazione,	raccolta presso interessati	Axios,

Descrizione generale delle misure di sicurezza adottate (se possibile):

- ✓ Gestione cartacea: presidio punti di stampa
- ✓ Controllo accesso locali amministrativi;
- ✓ Antivirus con controllo rete
- ✓ Procedure di backup e disaster recovery;
- ✓ Nomina per iscritto personale;
- ✓ Armadi chiusi;
- ✓ Nomina per iscritto responsabili esterni;
- ✓ Policy aziendali;
- ✓ Modifica credenziali;
- ✓ Programmazione della formazione del personale
- ✓ Rispetto normative anticendio
- ✓ Presenza presidi antincendio

Modalità di conservazione dei dati:

- ✓ Anaogico
- ✓ Digitale

Funzione di business/Unità Organizzativa/Dipartimento: Gestione alunni con disabilità

Denominazione del trattamento: Gestione alunni con disabilità

Finalità del trattamento	Software, Database, Manutenzione	Categorie di interessati	Categorie di dati personali	Categorie di destinatari a cui i dati sono o possono essere comunicati	Periodo di conservazione dei dati	Articolo 6 (base giuridica su cui si fonda il trattamento)	Articolo 9 (base giuridica per il trattamento di particolari categorie di dati)	Tipologia di trattamento	Fonte dei dati personali (se applicabile)	Denominazione responsabili esterni (se presenti)
Gestione alunni con disabilità	Axios SIDI	alunni-docenti-personale-famiglie	Dati identificativi della persona: Cognome, Nome, data di nascita, luogo di nascita, codice fiscale, residenza, domicilio, telefono, emai, dati relativi allo stato di salute	Altre Amministrazioni Pubbliche sulla base dell'interesse pubblico al trattamento, soggetti privati se previsto da norme di legge o regolamento	Termine delle finalità per le quali il dato è stato raccolto	Obbligo legale	Obbligo legale	Comunicazione, estrazione, copia, duplicazione, cancellazione, conservazione,	raccolta presso interessati	Axios,

Descrizione generale delle misure di sicurezza adottate (se possibile):

- ✓ Gestione cartacea: presidio punti di stampa
- ✓ Controllo accesso locali amministrativi;
- ✓ Antivirus con controllo rete
- ✓ Procedure di backup e disaster recovery;
- ✓ Nomina per iscritto personale;
- ✓ Armadi chiusi;
- ✓ Nomina per iscritto responsabili esterni;
- ✓ Policy aziendali;
- ✓ Modifica credenziali;
- ✓ Programmazione della formazione del personale
- ✓ Rispetto normative anticendio

✓ Presenza presidi antincendio
Modalità di conservazione dei dati: ✓ Anaogico ✓ Digitale

Funzione di business/Unità Organizzativa/Dipartimento: Gestione Sito scolastico

Denominazione del trattamento: Gestione sito scolastico

Finalità del trattamento	Software, Database, Manutenzione	Categorie di interessati	Categorie di dati personali	Categorie di destinatari a cui i dati sono o possono essere comunicati	Periodo di conservazione dei dati	Articolo 6 (base giuridica su cui si fonda il trattamento)	Articolo 9 (base giuridica per il trattamento di particolari categorie di dati)	Tipologia di trattamento	Fonte dei dati personali (se applicabile)	Denominazione responsabili esterni (se presenti)
Gestione sito scolastico	=	alunni-docenti-personale-famiglie	Dati personali	Altre Amministrazioni Pubbliche sulla base dell'interesse pubblico al trattamento, soggetti privati se previsto da norme di legge o regolamento	Termine delle finalità per le quali il dato è stato raccolto	l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;	l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;	Comunicazione, estrazione, copia, duplicazione, cancellazione, conservazione,	raccolta presso interessati	=

Descrizione generale delle misure di sicurezza adottate (se possibile):

- ✓ Gestione cartacea: presidio punti di stampa
- ✓ Controllo accesso locali amministrativi;
- ✓ Antivirus con controllo rete
- ✓ Procedure di backup e disaster recovery;
- ✓ Nomina per iscritto personale;
- ✓ Armadi chiusi;
- ✓ Nomina per iscritto responsabili esterni;
- ✓ Policy aziendali;
- ✓ Modifica credenziali;
- ✓ Programmazione della formazione del personale
- ✓ Rispetto normative anticendio
- ✓ Presenza presidi antincendio

Modalità di conservazione dei dati:

- ✓ Anaogico
- ✓ Digitale

Funzione di business/Unità Organizzativa/Dipartimento: Referente COVID

Denominazione del trattamento: attività ruolo referente covid

Finalità del trattamento	Software, Database, Manutenzione	Categorie di interessati	Categorie di dati personali	Categorie di destinatari a cui i dati sono o possono essere comunicati	Periodo di conservazione dei dati	Articolo 6 (base giuridica su cui si fonda il trattamento)	Articolo 9 (base giuridica per il trattamento di particolari categorie di dati)	Tipologia di trattamento	Fonte dei dati personali (se applicabile)	Denominazione responsabili esterni (se presenti)
Adempimento compiti del referente covid	Nessuno	alunni-docenti-personale-famiglie	Dati personali e sanitari	Dipartimento di prevenzione ASL.	Termine delle finalità per le quali il dato è stato raccolto	Obbligo legale il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;	Obbligo legale il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;	Comunicazione, estrazione, copia, duplicazione, cancellazione, conservazione,	raccolta presso interessati o attraverso il Dipartimene di prevenzione ASL o figure sanitarie	=

Descrizione generale delle misure di sicurezza adottate (se possibile):

- ✓ Gestione cartacea: presidio punti di stampa
- ✓ Controllo accesso locali amministrativi;
- ✓ Antivirus con controllo rete
- ✓ Procedure di backup e disaster recovery;
- ✓ Nomina per iscritto personale;
- ✓ Armadi chiusi;
- ✓ Nomina per iscritto responsabili esterni;
- ✓ Policy aziendali;
- ✓ Modifica credenziali;
- ✓ Programmazione della formazione del personale
- ✓ Rispetto normative anticendio
- ✓ Presenza presidi antincendio

Modalità di conservazione dei dati:

- ✓ Anaogico
- ✓ Digitale