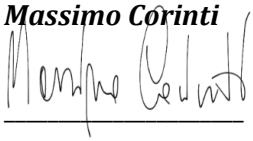
MPI - UFFICIO SCOLASTICO REGIONALE PER IL LAZIO
ISTITUTO COMPRENSIVO "TULLIO DE MAURO"
Viale Fernando Santi, 65 - 00155 ROMA - Tel. 06/ 95955067
Cod. Fisc.: 97567160581 – Cod. Mecc.: RMIC8B5008
E-mail: rmic8b5008@istruzione.it – PEC: rmic8b5008 @pec.istruzione.it

Registro delle attività di trattamento

Ex Art. 30 Regolamento UE 2016/679

STORIA DELLE VERSIONI		
Versione V1	04 ottobre 2022	Adozione del registro
Versione V2	27 ottobre 2022	Formazione del personale

Il Responsabile per la Protezione dei Dati Personali (DPO)
Massimo Corinti



Roma, lì 04 ottobre 2022

INDICE

1. SCOPO

Il presente Registro dei Trattamenti (di seguito "Registro") è adottato ai sensi dell'Art. 30 del Regolamento UE 2016/679 noto anche come GDPR "*General Data Protection Regulation"* in vigore dal 24 maggio 2016 (di seguito "Regolamento"), al fine di tracciare le attività di trattamento dei dati personali effettuati dall'Istituto Comprensivo Statale "Tullio De Mauro" di Roma, i criteri organizzativi adottati e le misure per la protezione dei dati personali

In particolare, il Registro dei Trattamenti contiene idonee informazioni riguardo:

- il nome e i dati di contatto del Titolare del trattamento del rappresentante del Titolare del trattamento e del Responsabile della Protezione dei Dati (RPD/DPO);
- le finalità del trattamento;
- una descrizione delle categorie di interessati e delle categorie di dati personali;
- le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
- ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
- ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

Il Registro è tenuto in forma scritta, anche in formato elettronico.

Su richiesta, il Titolare del trattamento mette il Registro a disposizione dell'autorità di controllo.

2. DEFINIZIONI

Ai fini del presente registro s'intende per:

1) «**dato personale**»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo on-line o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

2) «**trattamento**»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

3) «**limitazione di trattamento**»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

4) «**profilazione**»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

5) «**pseudonimizzazione**»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

6) «**archivio**»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

7) «**titolare del trattamento**»: 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;

8) «**responsabile del trattamento**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

9) «**destinatario**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

10) «**terzo**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

11) «**consenso dell'interessato**»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

12) «**violazione dei dati personali**»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

13) «**dati genetici**»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

14) «**dati biometrici**»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

15) «**dati relativi alla salute**»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

16) «**stabilimento principale**»:

a) per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale;
b) con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del Regolamento Europeo 2016/679;

17) «**rappresentante**»: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del **R**egolamento **Europeo 2016/679**;

18) «**impresa**»: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;

19) «**gruppo imprenditoriale**»: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;

20) «**norme vincolanti d'impresa**»: le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;

21) «**autorità di controllo**»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51; in Italia è il Garante per la Protezione dei Dati Personali, detto anche Garante della Privacy;

22) «**autorità di controllo interessata**»: un'autorità di controllo interessata dal trattamento di dati personali in quanto: il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo;

a) gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure
b) un reclamo è stato proposto a tale autorità di controllo;

23) «**trattamento transfrontaliero**»:

a) trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure
b) trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale interessati in più di uno Stato membro;

24) «**obiezione pertinente e motivata**»: un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del Regolamento Europeo 2016/679, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al Regolamento Europeo 2016/679, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà

fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione;

25) «**servizio della società dell'informazione**»: il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio;

26) «**organizzazione internazionale**»: un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.

3. TITOLARE DEL TRATTAMENTO

Il Titolare del Trattamento, (di seguito "Titolare") è l'Istituto Comprensivo Statale "Tullio De Mauro", con sede legale in Viale Fernando Santi, 65 - 00155 ROMA, nella persona del Dirigente Scolastico pro tempore.

Tel. +39 06/ 95955067, E-mail: rmic8b5008@istruzione.it - PEC: rmic8b5008@pec.istruzione.it

Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il Titolare del trattamento mette in atto misure tecniche e organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario.

Se ciò è proporzionato rispetto alle attività di trattamento, le misure includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento.

L'adesione ai codici di condotta di cui all'articolo 40 o a un meccanismo di certificazione di cui all'articolo 42 può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento.

4. RESPONSABILE PER LA PROTEZIONE DEI DATI PERSONALI (RPD/DPO)

Ai sensi dell'art. 37 del regolamento, il Titolare del trattamento designa sistematicamente un Responsabile della Protezione dei Dati personali (RPD) o anche Data Protection Officer (DPO) ogniqualvolta il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali.

Il Responsabile della Protezione dei Dati è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39.

Il responsabile della protezione dei dati assolvere i suoi compiti in base a un contratto di servizi.

Il Titolare del trattamento o il Delegato Interno al trattamento pubblica i dati di contatto del responsabile della protezione dei dati e li ha comunicati all'autorità di controllo in data 24 maggio 2018.

All'interno dell'Istituto, il Titolare ha stabilito il seguente Responsabile della Protezione dei Dati personali:

Tipo di designazione: Esterno - Persona: Fisica

Riferimenti:

Massimo Corinti
Codice fiscale CRNMSM65D28F499O – Partita iva 01961770565;
Sede Legale in Via Verentana 57 – 01027 Montefiascone (VT);
Domicilio Fiscale in Via Cremuzio Cordo – 00136 Roma (RM);
Cellulare: +39 335 7687380 - e-mail: dpo@corinti.eu - PEC dpo@pec.corinti.eu;

nel rispetto di quanto previsto dall'art. 39, par. 1, del GDPR è incaricato di svolgere, in piena autonomia e indipendenza, i seguenti compiti e funzioni:

a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal GDPR, nonché da altre disposizioni nazionali o dell'Unione Europea relative alla protezione dei dati;
b) sorvegliare l'osservanza del GDPR, di altre disposizioni nazionali o dell'Unione Europea relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35 del GDPR;
d) cooperare con il Garante per la protezione dei dati personali;

e) fungere da punto di contatto con il Garante per la protezione dei dati personali per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

5. DELEGATO INTERNO E ADDETTO AL TRATTAMENTO DEI DATI PERSONALI

Qualora un trattamento debba essere effettuato per conto del Titolare del trattamento, quest'ultimo ricorre ad un delegato, ovvero Responsabile del Trattamento Dati interno, che presenta garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.

Il Delegato Interno al trattamento non ricorre a un altro Delegato Interno senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il Delegato Interno al trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri Delegati Interni al trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche.

I trattamenti da parte di un Delegato Interno al trattamento sono disciplinati da una lettera di nomina a norma del diritto dell'Unione o degli Stati membri, che vincola il Delegato Interno al Titolare del trattamento e che indichi la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del Titolare del trattamento.

La lettera di nomina prevede, in particolare, che il Delegato Interno al trattamento:

a) tratti i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il Delegato Interno al trattamento; in tal caso, il Delegato Interno al trattamento informa il Titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;

b) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;

c) adotti tutte le misure richieste ai sensi dell'articolo 32 del regolamento: sicurezza del trattamento;

d) rispetti le condizioni di cui ai paragrafi 2 e 4 per ricorrere a un altro Delegato Interno al trattamento;

e) tenendo conto della natura del trattamento, assista il Titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del Titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo 16;

f) assista il Titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del regolamento, tenendo conto della natura del trattamento e delle informazioni a disposizione del Delegato Interno al trattamento;

g) su scelta del Titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati;

h) metta a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal Titolare del trattamento o da un altro soggetto da questi incaricato.

Con riguardo alla lettera h) del primo comma, il Delegato Interno al trattamento informa immediatamente il Titolare del trattamento qualora, a suo parere, un'istruzione violi il presente regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.

Quando il Delegato Interno al trattamento ricorre a un altro Delegato Interno al trattamento per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento, su tale altro Delegato Interno al trattamento sono imposti, mediante una nomina o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nella nomina o in altro atto giuridico tra il Titolare del trattamento e il Delegato Interno al trattamento di cui al paragrafo 3, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento. Qualora l'altro Delegato Interno al trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Delegato Interno al

trattamento iniziale conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro Delegato Interno al trattamento.

L'adesione da parte del Delegato Interno al trattamento a un codice di condotta approvato di cui all'articolo 40 del regolamento o a un meccanismo di certificazione approvato di cui all'articolo 42 del regolamento può essere utilizzata come elemento per dimostrare le garanzie sufficienti di cui ai paragrafi 1 e 4 del presente articolo.

Fatto salvo un contratto individuale tra il Titolare del trattamento e il Delegato Interno al trattamento, il contratto o altro atto giuridico di cui ai paragrafi 3 e 4 del presente articolo può basarsi, in tutto o in parte, su clausole contrattuali tipo di cui ai paragrafi 7 e 8 del presente articolo, anche laddove siano parte di una certificazione concessa al Titolare del trattamento o al Delegato Interno al trattamento ai sensi degli articoli 42 e 43 del regolamento.

La Commissione può stabilire clausole contrattuali tipo per le materie di cui ai paragrafi 3 e 4 del presente articolo e secondo la procedura d'esame di cui all'articolo 93, paragrafo 2.

Un'autorità di controllo può adottare clausole contrattuali tipo per le materie di cui ai paragrafi 3 e 4 del presente articolo in conformità del meccanismo di coerenza di cui all'articolo 63.

Il contratto o altro atto giuridico di cui ai paragrafi 3 e 4 è stipulato in forma scritta, anche in formato elettronico.

Fatti salvi gli articoli 82, 83 e 84, se un Delegato Interno al trattamento viola il presente regolamento, determinando le finalità e i mezzi del trattamento, è considerato un Titolare del trattamento in questione.

All’interno della sua organizzazione, il Titolare ha stabilito i seguenti Delegati Interni al trattamento dei dati (Allegato Testo completo della nomina):

Identificativo	Funzione/Incarico	Modalità
xxx	DSGA	Nomina

L’ incaricato di trattamento, è tenuto ad attenersi scrupolosamente alle istruzioni fornite dal Titolare o dal Responsabile, anche in materia di sicurezza, riportate nei documenti aziendali (es.: regolamenti e manuali operativi) messi a Sua disposizione, il mancato rispetto di tali istruzioni – come da allegato - potrà comportare la violazione degli obblighi previsti dalla normativa Privacy ed esporre il Titolare, i relativi esponenti ed anche i singoli incaricati a rischi sul piano delle responsabilità e delle sanzioni a livello civile, amministrativo e, nei casi più gravi, anche penale.

All’interno della sua organizzazione, ai sensi dell’art. 2-quaterdecies del d.lgs. 196/2003 come novellato dal d.lgs. 101/2018, il Titolare ha stabilito con nomina i seguenti **Addetti Interni al trattamento dei dati**:

Identificativo	Identificativo	Identificativo

6. DATI TRATTATI

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

6.1. Natura dei dati trattati.

La natura dei dati soggetti al trattamento da parte della scuola è la seguente:

a) Documentazioni complete riguardanti gli alunni, relativi al corso di studi, alla presenza di diversamente abili, 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;
b) Documenti eventualmente prodotti dalle famiglie anche riguardanti la certificazione della situazione patrimoniale e delle condizioni economiche.
c) 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;
d) Dati per gestire le negoziazioni e le relative modalità di pagamento per la fornitura di beni e servizi;
e) Dati contabili e fiscali;

Nel trattamento dei dati di natura **sensibile e giudiziaria**, così come definiti dall'art. 4 del regolamento 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".

6.2. Banche dati attivate.

Le banche dati attivate sono quelle di seguito riportate:

- Alunni
- Dipendenti
- Protocollo
- Inventario
- Magazzino
- Registro Conto Corrente Postale
- Fornitori
- Bilancio
- Retribuzioni
- Registro di classe
- Registro degli insegnanti
- Pago in Rete
- Registro infortuni alunni e dipendenti

6.3. Finalità perseguita con il trattamento dei dati.

Nell'ambito della propria funzione istituzionale l'Istituto scolastico tratta dati personali di studenti, personale dipendente e fornitori per le seguenti finalità:

- Garanzia del servizio scolastico
- Gestione e formazione del personale
- Adempimenti assicurativi
- Certificazione degli esiti scolastici e dei servizi prestati dai dipendenti
- Acquisizione di beni e servizi da terzi fornitori
- Attività strumentali alle precedenti

6.4. Affidamento dei dati a terzi per il trattamento.

Tutti i dati posseduti dall'Istituto vengono trattati esclusivamente presso gli Uffici dell'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 e in seguito ad esplicito consenso espresso dagli stessi.

6.5. Modalità di trattamento.

La conservazione ed il trattamento dei dati viene effettuata nel modo seguente:

Cartaceo:

I dati in possesso dell'Istituto sono conservati in locali e armadi dotati di chiusura a chiave ai quali hanno accesso esclusivamente i soggetti autorizzati. 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.

Mediante il 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.

7. ELENCO DEI TRATTAMENTI (TR.) DI DATI PERSONALI. TABELLA RIASSUNTIVA

Identificativo del Trattamento		Struttura di riferimento	Altre strutture concorrenti al trattamento	Descrizione degli strumenti utilizzati
TR.1	**Selezione e reclutamento a tempo indeterminato e determinato, e gestione del rapporto di lavoro del personale dipendente, ecc.**	Dirigente Scolastico, DSGA e Segreteria Amministrativa (e assimilati)	Collaboratori del D.S., Collaboratori scolastici, RSPP e addetti SPP, Medico Competente	Documenti cartacei, registri e strumenti elettronici
TR.2	**Dipendenti e assimilati: gestione del contenzioso e procedimenti disciplinari**	Dirigente Scolastico, DSGA e Segreteria Amministrativa (e assimilati)	-	Documenti cartacei e strumenti elettronici
TR.3	**Organismi collegiali e commissioni istituzionali**	Dirigente Scolastico, DSGA e Segreteria Amministrativa (e assimilati)	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**	Dirigente Scolastico, DSGA e Segreteria Amministrativa (e assimilati)	Collaboratori del D.S., Funzioni Strumentali, Docenti, Collaboratori scolastici	Documenti cartacei, registri e strumenti elettronici
TR.5	**Attività educativa, didattica e formativa, di**	Dirigente Scolastico, DSGA e Segreteria	Collaboratori del D.S., Funzioni Strumentali,	Documenti cartacei, registri e strumenti

	valutazione	Amministrativa (e assimilati)	Docenti, Collaboratori scolastici, membri esterni organi collegiali	elettronici
TR.7	**Rapporti scuola - famiglie e gestione del contenzioso**	Dirigente Scolastico, DSGA e Segreteria Amministrativa (e assimilati), Docenti	-	Documenti cartacei e strumenti elettronici
TR.8	**Fornitori e clienti**	Dirigente Scolastico, DSGA e Segreteria Amministrativa (e assimilati)	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 (e assimilati)	Collaboratori del D.S	Documenti cartacei, registri e strumenti elettronici
TR.10	**Gestione Istituzionale**	Dirigente Scolastico, DSGA e Segreteria Amministrativa (e assimilati)	Collaboratori del D.S	Documenti cartacei, registro protocollo, e strumenti elettronici
TR.11	**Gestione sito web dell'istituto**	Dirigente Scolastico, Incaricati sito web	docente incaricato	Documenti cartacei e strumenti elettronici

8. TRATTAMENTI TR.1 E TR.2	
TR.1	**Selezione e reclutamento a tempo indeterminato e determinato, e gestione del rapporto di lavoro del personale dipendente, ecc.**
TR.2	**Dipendenti e assimilati: gestione del contenzioso e procedimenti disciplinari**

(In Allegato 7 le Informazioni fornite ai Dipendenti sul trattamento dei dati personali)

8.1 Categorie di Interessati.

- Personale docente, personale dipendente a tempo determinato e indeterminato

8.2 Categorie di Dati Personali.

- Dati anagrafici degli insegnanti a tempo indeterminato, insegnanti a tempo determinato, insegnanti esterni incaricati di funzioni nella scuola: nome, cognome, indirizzo, numeri di telefono, di telefax, indirizzo di posta elettronica, ecc.;
- dati dei familiari degli insegnanti a tempo indeterminato, insegnanti a tempo determinato, insegnanti esterni incaricati di funzioni nella scuola;

- dati relativi alle assenze per malattia;
- dati relativi alle assenze per permessi familiari (congedi parentali) e per ragioni di studio/formazione/aggiornamento;
- dati relativi ai permessi per familiari diversamente abili riconosciuto (Legge 104/92, L. 53/2000);
- dati relativi ai permessi per maternità/paternità;
- dati relativi ai permessi sindacali/amministrativi;
- dati relativi alle ferie;
- dati relativi all'analisi della situazione di carriera (certificato di servizio e dichiarazione dei servizi prestati);
- contratti di lavoro;
- dati inerenti alla retribuzione/stipendi (dati bancari);
- titoli di studio, dati sul grado di istruzione;
- dati relativi alle altre attività eventualmente svolte dal personale docente;
- comunicazioni al personale necessarie alla gestione amministrativa del rapporto lavorativo (lettere, circolari, avvisi, ecc.);
- dati relativi alla gestione del contenzioso e dei procedimenti disciplinari;
- convocazioni in tribunale;
- dati relativi ai permessi per la donazione del sangue;
- dati relativi ai permessi non retribuiti per i supplenti;
- dati relativi ai permessi previsti dagli artt. 15, 16 DEL CCNL 29/11/07;
- dati necessari per attivare gli organismi collegiali e le commissioni istituzionali previsti dalle norme di organizzazione del Ministero della Pubblica Istruzione e dell'ordinamento scolastico;
- dati relativi alla partecipazione a scioperi;
- dati relativi alla partecipazione ad assemblee sindacali.

8.3 Natura dei dati.

I dati trattati sono personali anche di categorie particolari "c.d. **sensibili"** (dati idonei a rivelare le convinzioni religiose, filosofiche, sindacali, d'altro genere; dati idonei a rivelare lo stato di salute, in relazione alle patologie attuali e/o pregresse e alle terapie in corso; dati relativi alle procedure per la selezione e il reclutamento, all'instaurazione, alla gestione e alla cessazione del rapporto di lavoro; gestione del contenzioso e procedimenti disciplinari; dati idonei a rivelare la vita sessuale, esclusivamente in caso di rettificazione di attribuzione di sesso) e di categorie particolari **"**giudiziari**"** per la gestione del contenzioso e procedimenti disciplinari).

Il trattamento concerne tutti i dati relativi alle procedure per la selezione e il reclutamento, all'instaurazione, alla gestione e alla cessazione del rapporto di lavoro.

I dati inerenti lo stato di salute sono trattati per: l'adozione di provvedimenti di stato giuridico ed economico, verifica dell'idoneità al servizio, assunzioni del personale appartenente alle c.d. categorie protette, benefici previsti dalla normativa in tema di assunzioni, protezione della maternità, igiene e sicurezza sul luogo di lavoro, causa di servizio, equo indennizzo, onorificenze, svolgimento di pratiche assicurative pensionistiche, e previdenziali obbligatori e contrattuali, trattamenti assistenziali, riscatti e ricongiunzioni previdenziali, denunce di infortuni e/o sinistri e malattie professionali, fruizione di assenze, particolari esenzioni o permessi lavorativi per il personale e provvidenze, collegati a particolari condizioni di salute dell'interessato o dei suoi familiari, assistenza fiscale, mobilità territoriale, professionale e intercompartimentale;

I dati idonei a rilevare l'adesione a sindacati o ad organizzazioni di carattere sindacale per gli adempimenti connessi al versamento delle quote di iscrizione o all'esercizio dei diritti sindacali;

I dati idonei sulle convinzioni religiose per la concessione di permessi per festività oggetto di specifica richiesta dell'interessato motivata per ragioni di appartenenza a determinate confessioni religiose. I dati sulle convinzioni religiose vengono in rilievo anche ai fini del reclutamento dei docenti di religione.

I dati sulle convinzioni filosofiche o d'altro genere possono venire in evidenza dalla documentazione connessa allo svolgimento del servizio di leva come obiettore di coscienza;

I dati di carattere giudiziario sono trattati nell'ambito delle procedure concorsuali al fine di valutare il possesso dei requisiti di ammissione e per l'adozione dei provvedimenti amministrativo contabili connessi a vicende giudiziarie che coinvolgono l'interessato.

Le informazioni sulla vita sessuale possono desumersi unicamente in caso di eventuale rettificazione di attribuzione di sesso.

8.4 Destinatari.

- MPI, Ufficio Scolastico Regionale, Ufficio Scolastico Provinciale;
- Altri Istituti Scolastici, Enti di formazione;
- Ufficio di Collocamento (dati dei supplenti, dati anagrafici, dati sul grado d'istruzione, durata della supplenza);
- Direzione Provinciale dei Servizi Vari (tesoreria), Ragioneria Provinciale dello Stato;
- INPS, INDIRE, Ministero dell'Economia; sindacati che con domanda motivata richiedano dati relativi ad attività esclusivamente connessa alle loro funzioni;
- Assicurazioni private, INAIL, Revisore contabile, A.S.S.;
- Musei, teatri, agenzie di viaggi, fondazioni;
- Comune, Provincia, Regione ed altri Enti Pubblici, anche per il personale assunto obbligatoriamente ai sensi della L. 68/1999;
- Servizi sanitari competenti per le visite fiscali e per l'accertamento dell'idoneità all'impiego;
- Organi preposti al riconoscimento della causa di servizio/equo indennizzo» ai sensi del DPR 461/2001;
- Organi preposti alla vigilanza in materia di igiene e sicurezza sui luoghi di lavoro (D.lg. n. 81/2008)
- Enti assistenziali, previdenziali e assicurativi, autorità di pubblica sicurezza a fini assistenziali e previdenziali, nonché per la denuncia delle malattie professionali o infortuni sul lavoro ai sensi del DPR. n. 1124/1965;
- Organizzazioni sindacali per gli adempimenti connessi al versamento delle quote di iscrizione e per la gestione dei permessi sindacali;
- Pubbliche Amministrazioni presso le quali vengono comandati i dipendenti, o assegnati nell'ambito della mobilità;
- Ordinario Diocesano per il rilascio dell'idoneità all'insegnamento della Religione Cattolica ai sensi della Legge 18 luglio 2003, n. 186;
- Organi di controllo (Corte dei Conti e MEF): al fine del controllo di legittimità e annotazione della spesa dei provvedimenti di stato giuridico ed economico del personale ex Legge n. 20/94 e DPR 20 febbraio 1998, n.38; Agenzia delle Entrate: ai fini degli obblighi fiscali del personale ex Legge 30 dicembre 1991, n. 413;
- MEF e INPDAP: per la corresponsione degli emolumenti connessi alla cessazione dal servizio ex Legge 8 agosto 1995, n. 335.
- Presidenza del Consiglio dei Ministri per la rilevazione annuale dei permessi per cariche sindacali e funzioni pubbliche elettive (art. 50, comma 3, D.lg. n.165/2001);
- Ministero del Lavoro e delle Politiche Sociali: per lo svolgimento dei tentativi obbligatori di conciliazione dinanzi a Collegi di conciliazione ex D.Lgs. 30 marzo 2001, n. 165;
- Organi arbitrali: per lo svolgimento delle procedure arbitrali ai sensi dei CCNL di settore;
- Avvocature dello Stato: per la difesa erariale e consulenza presso gli organi di Giustizia;
- Magistrature ordinarie e amministrative-contabile e Organi di Polizia Giudiziaria per l'esercizio dell'azione di giustizia;
- Liberi professionisti, ai fini di patrocinio o di consulenza, compresi quelli di controparte per le finalità di corrispondenza sia in fase giudiziale che stragiudiziale.

8.5 Trasferimenti di dati verso un paese terzo.

I dati non sono trasferiti verso un paese terzo o verso un'organizzazione internazionale.

8.6 Durata del trattamento.

I dati sono di norma conservati per un periodo non superiore a quello necessario al conseguimento delle finalità per la quali sono stati raccolti.

9. TRATTAMENTI TR.4, TR.5, E TR.7	
TR.4	**Attività propedeutiche all'avvio dell'anno scolastico**
TR.5	**Attività educativa, didattica e formativa, di valutazione**
TR.7	**Rapporti scuola - famiglie e gestione del contenzioso**

9.1 Categorie di Interessati.

- Alunni, ex-alunni, genitori

9.2 Categorie di Dati Personali.

- Dati anagrafici degli alunni: nome, cognome, indirizzo, numeri di telefono, di telefax, indirizzo di posta elettronica, ecc.
- Dati personali dei familiari degli alunni;
- Dati relativi alle assenze;
- Certificati medici;
- Valutazione dell'alunno;
- Diplomi ed attestati;
- Scelta relativa all'ora di religione;
- Curriculum scolastico (promozioni, bocciature);
- Comunicazioni tra scuola e studente/famiglia dello studente;
- Tasse scolastiche (esoneri);
- Dati relativi alla gestione del contenzioso;
- Dati relativi ad eventuali diversamente abili;
- Lettere e comunicazioni alle famiglie;
- Fotografie, riprese audio-video (eventuali).

I dati sopra descritti riguardano anche gli ex allievi dell'Istituto: tali dati sono conservati per il periodo previsto dalla legge.

9.3 Natura dei dati.

I dati trattati sono personali anche di categorie particolari sensibili (dati idonei a rivelare l'origine razziale o etnica, per favorire l'integrazione degli alunni stranieri; dati idonei a rivelare le convinzioni religiose, per garantire la libertà di credo religioso e per la fruizione dell'insegnamento della religione cattolica o delle attività alternative a tale insegnamento; dati idonei a rivelare le convinzioni filosofiche, politiche, d'altro genere, per la costituzione e il funzionamento delle Consulte e delle Associazioni degli studenti e dei familiari; dati idonei a rivelare lo stato di salute, in relazione alle patologie attuali e/o pregresse e alle terapie in corso, per assicurare l'erogazione del sostegno agli alunni disabili, dell'insegnamento domiciliare ed ospedaliero nei confronti degli alunni affetti da gravi patologie, per la partecipazione alle attività educative e didattiche programmate a quelle motorie e sportive, alle visite guidate e ai viaggi d'istruzione, all'erogazione del servizio mensa) e particolari a carattere giudiziario (nel caso in cui l'autorità giudiziaria abbia predisposto un programma di protezione nei confronti dell'alunno e/o della famiglia dell'alunno, oppure per la gestione del contenzioso con le famiglie degli alunni).

9.4 Destinatari.

- MPI, Ufficio Scolastico Provinciale, Ufficio Scolastico Regionale;
- Assicurazioni private, INAIL;
- Consolati, direttori centri cultura esteri;
- Musei, teatri, agenzie di viaggi, fondazioni;
- Procura della Repubblica, Tribunale dei minori, Tribunale;
- Comune, Provincia, Regione ed altri Enti Pubblici per la fornitura dei servizi ai sensi del D.Lgs.. 31 marzo 1998, n. 112, limitatamente ai dati indispensabili all'erogazione del servizio;
- S.I.D.D.I.F. - Sistema informativo per il Diritto/Dovere all'Istruzione e alla Formazione (contenente l'Anagrafe degli studenti e l'Osservatorio sulla scolarità);

- Gestori pubblici e privati dei servizi di assistenza agli alunni e di supporto all'attività scolastica, ai sensi delle leggi regionali sul diritto allo studio, limitatamente ai dati indispensabili all'erogazione del servizio;
- Altri Istituti Scolastici, statali e non enti di formazione;
- Aziende, imprese e altri soggetti pubblici e/o privati per tirocini formativi, stage e alternanza scuola-lavoro ai sensi della Legge 24 giugno 1997, n. 196 e del D.Lgs.. 21 aprile 2005 n. 77 e, facoltativamente, per attività di rilevante interesse sociale ed economico, limitatamente ai dati indispensabili all'erogazione dei servizi;
- Associazioni Sportive, Professionisti (per specifici progetti);
- Avvocature dello Stato: per la difesa erariale e consulenza presso gli organi di Giustizia;
- Magistrature ordinarie e amministrative-contabile e Organi di polizia giudiziaria per l'esercizio dell'azione di giustizia;
- Liberi professionisti, ai fini di patrocinio o di consulenza, compresi quelli di controparte per le finalità di corrispondenza sia in fase giudiziale che stragiudiziale.

9.5 Trasferimenti di dati verso un paese terzo.

I dati non sono trasferiti verso un paese terzo o verso un'organizzazione internazionale.

9.6 Durata del trattamento.

I dati sono di norma conservati per un periodo non superiore a quello necessario al conseguimento delle finalità per la quali sono stati raccolti, e in ottemperanza a quanto prescritto dalla Soprintendenza Archivistica Regionale.

10. TRATTAMENTI TR.3, TR.8, TR.9 E TR.10	
TR.3	**Organismi collegiali e commissioni istituzionali**
TR.8	**Fornitori e Clienti**
TR.9	**Gestione finanziaria e contabile**
TR.10	**Gestione Istituzionale**

10.1 Categorie di Interessati.

- Fornitori, Clienti, Collaboratori, Professionisti, Banche, etc., Enti

10.2 Categorie di Dati Personali.

- Dati anagrafici: nome, cognome, indirizzo, numeri di telefono, indirizzo di posta elettronica, codice fiscale, partita iva, ecc.
- Coordinate Bancarie

10.3 Natura dei dati.

I Dati verranno trattati per l'effettuazione di adempimenti amministrativo-contabili, quali la gestione della contabilità e della tesoreria, nonché la fatturazione (ad esempio la verifica e la registrazione delle fatture), in conformità a quanto richiesto dalla normativa vigente, o per l'esecuzione di altri obblighi previsti da leggi, da regolamenti e dalla normativa comunitaria.

10.4 Destinatari.

- Istituti Pubblici stabiliti dalla legge e più in generale da tutti gli Enti previsti dalla vigente normativa in materia contabile e fiscale come destinatari di comunicazioni obbligatorie;
- MPI, Ufficio Scolastico Provinciale, Ufficio Scolastico Regionale;
- Altri Istituti Scolastici, statali e non, enti di formazione;
- Avvocature dello Stato: per la difesa erariale e consulenza presso gli organi di Giustizia;
- Magistrature ordinarie e amministrative-contabile e Organi di polizia giudiziaria per l'esercizio dell'azione di giustizia;
- Liberi professionisti, ai fini di patrocinio o di consulenza, compresi quelli di controparte per le finalità di corrispondenza sia in fase giudiziale che stragiudiziale.

10.5 Trasferimenti di dati verso un paese terzo.
I dati non sono trasferiti verso un paese terzo o verso un'organizzazione internazionale,

10.6 Durata del trattamento.
I dati sono di norma conservati per un periodo non superiore a quello necessario al conseguimento delle finalità per la quali sono stati raccolti.

11. 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:

STRUTTURA:	TRATTAMENTI OPERATI DALLA STRUTTURA:	COMPITI DELLA STRUTTURA:
DIRIGENTE SCOLASTICO:	Tutti	Direzione generale di tutte le attività, gestione delle pratiche riservate.
SOGGETTI AUTORIZZATI INTERNI, UNITA' ORGANIZZATIVE OMOGENEE: (Testo completo delle nomine negli allegati 4 e 5)		
Collaboratori del DS	Tutti	Affiancamento al D.S. con deleghe parziali e sostituzione dello stesso in caso di assenza
Segreteria	Tutti Tr .3 anche dati sindacali. In casi eccezionali: Tr.1, Tr.5 (dati sensibili). Se membri di commissione Tr.2 (dati sensibili o giudiziari)	Gestione amministrativa di tutte le pratiche e supporto al Dirigente Scolastico e al Corpo Docente
Corpo Docente	Tr.3, Tr.4, Tr.5, Tr.7, Tr.8, Tr.9, Tr.10. Tr .3 anche dati sindacali. In casi eccezionali: Tr.1, Tr.5 (dati sensibili). Se membri di commissione Tr.2 (dati sensibili o giudiziari).	Insegnamento e attività integrative e collaterali, partecipazione alle scelte organizzative e di orientamento generale, partecipazione alla gestione di specifiche attività (Biblioteca, scelte degli acquisti, commissioni varie, ecc.)
Collaboratori scolastici e personale ausiliario	Tutti, ma con attività di supporto. Tr .3 anche dati sindacali. In casi eccezionali: Tr.1, Tr.5 (dati sensibili). Se membri di commissione Tr.2 (dati sensibili o giudiziari).	Apertura e chiusura della sede, custodia e controllo, consegna e ricezione plichi e lettere, pulizia, assistenza a tutte le altre attività, gestione di dati comuni di alunni, docenti e familiari.
Membri ESTERNI di Organi Collegiali	Tr.3 e tutti gli altri (tranne Tr.6) limitatamente alle strette esigenze della funzione	Partecipazione alle attività gestionali e alle scelte organizzative e di orientamento generale, nonché il CDI e la GE decisioni di tipo amministrativo, finanziario, regolamentare
INCARICATI INTERNI CON COMPITI SPECIFICI O ULTERIORI:		

Backup eseguito in modalità automatica	Addetti limitatamente alla funzione	Il backup degli archivi informatici contenenti dati personali viene eseguito due volte la settimana in modalità automatica
STRUTTURA:	**TRATTAMENTI OPERATI DALLA STRUTTURA:**	**COMPITI DELLA STRUTTURA:**
Gestione delle password: DSGA	DSGA ma limitatamente alla funzione	Da ogni Incaricato munito di accesso al computer mediante password, ad ogni scadenza della password (3 o 6 mesi, a seconda dei casi) riceve una busta chiusa contenente la password, o inviata via mail da cambiare al primo accesso
Tecnico della Manutenzione del Software: xxx	Manutenzione hardware, monitoraggio dei sistemi con particolare riguardo alla sicurezza informatica, assistenza e manutenzione reti lan e wlan, installazione, configurazione, diagnostica sistemi operativi, controllo antivirus, migrazione dati, gestione backup	Manutenzione del software e piccoli interventi sull'hardware
R.S.P.P.: xxx R.L.S., Addetti al S.P.P. – Referenti Covid – Medico Competente	Trattamenti relativi all'applicazione della normativa sulla sicurezza (attualmente Testo unico D.Lgs.. 81/08) o ad essa riferiti. Trattamenti autorizzati: tutti i trattamenti informatici e non, rigorosamente nei limiti relativi alle funzioni, in particolare: Tr.1 Selezione e reclutamento a tempo indeterminato e determinato, e gestione del rapporto di lavoro del personale dipendente ecc. Tr.2 Dipendenti e Assimilati: Gestione del contenzioso e procedimenti disciplinari Tr.3 Organismi collegiali e commissioni istituzionali Tr.4 Attività propedeutiche all' avvio dell'anno scolastico Tr.5 Attività educativa, didattica e formativa, di valutazione	Applicazione normativa D.Lgs. 81/2008 e norme collegate; gestione sicurezza sul posto di lavoro e nella scuola in generale.
RLS - Rappresentante dei Lavoratori per la Sicurezza: xxx	Diritto di consultazione di tutti i documenti e materiali informatici strettamente inerenti alla funzione e risultanti come diritto di conoscenza	Contributo all'applicazione normativa D.Lgs. 81/2008 e norme collegate; gestione sicurezza sul posto di lavoro e nella scuola in generale; verifica

		ecc.
Docenti Incaricati della redazione e gestione di Piani Educativi Individuali xxx	Tutti i trattamenti informatizzati e relativi all'attività: Tr.4 Attività propedeutiche all' avvio dell'anno scolastico Tr.5 Attività educativa, didattica e formativa, di valutazione	Gestione di alunni diversamente abili di livello didattico grave.
Personale incaricato della creazione e/o gestione editoriale del sito web	I trattamenti informatici, rigorosamente nei limiti relativi alle seguenti funzioni: Tr.11 Gestione sito web dell'istituto	Creazione e/o gestione editoriale del sito web dell'Istituto.
STRUTTURA:	**TRATTAMENTI OPERATI DALLA STRUTTURA:**	**COMPITI DELLA STRUTTURA:**
DELEGATO INTERNO AL TRATTAMENTO:		
Direttore Servizi Generali Amministrativi (DSGA) :	Tutti i trattamenti, limitatamente alla gestione amministrativo- contabile e alla gestione delle attività del personale ATA	Gestione amministrativa di tutte le pratiche e supporto al Dirigente Scolastico e al Corpo Docente.
RESPONSABILI ESTERNI:		
R.S.P.P o Addetto al S.P.P. ai sensi del D.Lgs. 81/2008: xxx	I trattamenti relativi all'applicazione della normativa 81/2008 o ad essa riferiti. Trattamenti autorizzati: tutti i trattamenti informatici e non, rigorosamente nei limiti relativi alle funzioni, in particolare: Tr.1 Selezione e reclutamento a tempo indeterminato e determinato, e gestione del rapporto di lavoro del personale dipendente ecc. Tr.2 Dipendenti e Assimilati: Gestione del contenzioso e procedimenti disciplinari Tr.3 Organismi collegiali e commissioni istituzionali Tr.4 Attività propedeutiche all' avvio dell'anno scolastico Tr.5 Attività educativa, didattica e formativa, di valutazione	Applicazione normativa D.Lgs. 81/2008 e norme collegate; gestione sicurezza sul posto di lavoro e nella scuola in generale.
Axios Italia Service s.r.l. (per l'applicativo axios italia service)	Tutti i trattamenti informatici, rigorosamente nei limiti relativi alle funzioni	Manutenzione del software dei computer.
STRUTTURA:	**TRATTAMENTI OPERATI DALLA STRUTTURA:**	**COMPITI DELLA STRUTTURA:**

RESPONSABILI ESTERNI:		
Tecnico Esterno della Manutenzione dell'Hardware:	Tutti i trattamenti informatici, rigorosamente nei limiti relativi alle funzioni	Manutenzione dell'hardware dei computers.
Docente o animatore Esterno:	i seguenti trattamenti non informatici: Tr.4 - Attività propedeutiche all' avvio dell'anno scolastico; Tr.5 - Attività educativa, didattica e formativa, di valutazione, rigorosamente nei limiti relativi alle funzioni	Attività di animazione a favore degli alunni della scuola.
Tecnico esterno per la creazione e gestione del sito web: xxx	Trattamenti informatici, rigorosamente nei limiti relativi alle seguenti attività: Tr.11 Gestione sito web dell'istituto	Creazione e gestione redazionale del sito web dell'Istituto.
Agenzia viaggi: non previsti al momento viaggi di istruzione	Trattamenti informatici e non, rigorosamente nei limiti relativi alle funzioni: tr.5 - Attività educativa, didattica e formativa, di valutazione, ma limitatamente a pochissimi dati tr.1 – Gestione del personale, in quanto accompagnatori, ma limitatamente a pochissimi dati	Organizzazione di visite d'istruzione e viaggi.
Gestori di trasporti: non previsti al momento viaggi di istruzione	Trattamenti informatici e non, rigorosamente nei limiti relativi alle funzioni: tr.5 - Attività educativa, didattica e formativa, di valutazione, ma limitatamente a pochissimi dati tr.1 – Gestione del personale, in quanto accompagnatori, ma limitatamente a pochissimi dati	Organizzazione di visite d'istruzione e viaggi.
Ente di certificazione di qualità: xxx	Trattamenti informatici e non, rigorosamente nei limiti relativi alle funzioni.	Verifica delle condizioni che consentono l'ottenimento del marchio di qualità.
AMMINISTRATORE DI SISTEMA:		
Amministratore del sistema informatico: xxx	Tutti i trattamenti informatici, ma rigorosamente nei limiti della funzione.	Gestione del sistema informatico dell'istituto.

12. MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE.

Si riportano di seguito una sintesi delle misure di sicurezza tecniche ed organizzative adottate per la protezione dei dati personali trattati dall'amministrazione scolastica. Ulteriori misure di sicurezza di natura informatica sono riportate nel documento redatto dall'amministrazione scolastica secondo quanto previsto dalla circolare AGID 18 aprile 2017 n.2 - "Misure minime di sicurezza ICT per le pubbliche amministrazioni".

12.1 Protezione delle aree e dei locali

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, tutti i locali e armadi sono dotati di serrature a chiave.

L'ubicazione delle stampanti non consente ad estranei di leggere od asportare eventualmente documenti non ancora prelevati dal personale.

Il personale amministrativo, nominato tutto come soggetto autorizzato al 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.

12.2 Protezione dei supporti cartacei

Relativamente ai supporti cartacei, i criteri di protezione dei dati sono i 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;

- L'Istituto è dotato di distruggi documenti.

12.3 Trattamenti con l'ausilio di sistemi informatici

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 due dischi rigidi in configurazione RAID 1, configurazione 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 di Sistema che dovrà procedere all'immediata duplicazione degli archivi del disco e alle operazioni necessarie al ripristino o alla sostituzione del disco difettoso.

I soggetti autorizzati al 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.

12.4 Sistema di autenticazione e autorizzazione

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

Per quanto riguarda il sistema di autorizzazione, a ciascun Soggetto Autorizzato al 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.

In caso si debba accedere, per motivi di manutenzione tecnica o per lavoro, alla postazione dell'addetto in sua assenza, l'amministratore di sistema provvede a modificare la parola chiave dell'addetto e a comunicare la nuova parola chiave al tecnico informatico o al collega che sostituisce l'addetto. Al ritorno, l'addetto non potrà accedere al sistema e dovrà farsi dire la nuova parola chiave. Una volta avuto accesso al sistema, potrà di nuovo modificarsi la parola chiave in modo da renderla di nuovo riservata.

L'amministratore di sistema si assicura che le credenziali di autenticazione non utilizzate da almeno sei mesi siano disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica. Si assicura che le credenziali siano disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.

Ad ogni addetto al trattamento possono essere assegnate o associate individualmente una o più credenziali per l'autenticazione.

La parola chiave è composta da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'incaricato o al codice di accesso assegnato (user-id). La parola chiave è modificata dall'incaricato del trattamento al primo utilizzo e, successivamente, almeno ogni sei mesi o ogni tre mesi in caso di trattamento di particolari categorie di dati.

Gli addetti adottano le necessarie cautele per assicurare la segretezza della parola chiave. In particolare, è fatto divieto comunicare a chiunque altro addetto le proprie credenziali di accesso al sistema informatico.

Gli addetti hanno l'obbligo di non lasciare incustodito il proprio posto di lavoro e di prendere i necessari accorgimenti per evitare che, durante la loro assenza anche breve, altri addetti o persone non autorizzate possano accedere alla postazione di lavoro.

12.5 Smaltimento rifiuti apparecchiature elettroniche e misure di sicurezza dei dati personali.

Viste le disposizioni del Garante contenute nel provvedimento n° 287 del 09/12/2008 dal titolo "Rifiuti di apparecchiature elettroniche e misure di sicurezza dei dati personali", nello smaltimento dei PC in disuso verranno adottate specifiche misure che garantiscano l'impossibilità di accedere ai dati contenuti nei supporti di memoria.
Tale misura, non necessaria nei PC utilizzati per lo svolgimento dell'attività didattica e non contenenti dati personali, dovrà essere rigorosamente adottata per i PC utilizzati per lo svolgimento dell'attività amministrativa.

12.6 Criteri per garantire la sicurezza e la resilienza dei sistemi e dei dati personali.

All'amministratore di sistema è affidato il compito di verificare la situazione delle apparecchiature hardware e software installate con cui vengono trattati i dati, delle apparecchiature periferiche, ed in particolare dei dispositivi di collegamento con le reti pubbliche.

La verifica ha lo scopo di controllare l'affidabilità del sistema, per quanto riguarda:

- la sicurezza dei dati trattati
- il rischio di distruzione o di perdita

• il rischio di accesso non autorizzato o non consentito tenendo conto anche dell'evoluzione tecnologica, tenendo in particolare conto di:

- disponibilità di nuove versioni migliorative dei Sistemi operativi utilizzati;
- segnalazioni di Patch, Fix o System-Pack per la rimozione di errori o malfunzionamenti;

- segnalazioni di Patch, Fix o System-Pack per l'introduzione di maggiori sicurezze contro i rischi di intrusione o di danneggiamento dei dati o disponibilità di nuove versioni migliorative delle applicazioni installate che consentano maggiore sicurezza contro i rischi di intrusione o di danneggiamento dei dati.

Nel caso in cui esistano rischi evidenti l'amministratore di sistema deve informarne il Titolare del trattamento perché siano presi gli opportuni provvedimenti allo scopo di assicurare il corretto trattamento dei dati in conformità alle norme in vigore.

12.7 Protezione da virus informatici.

Al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita di dati a causa di virus informatici, il Titolare del trattamento dei dati stabilisce, con il supporto tecnico dell'amministratore di sistema, quali protezioni software adottare in relazione all'evoluzione tecnologica dei sistemi disponibili sul mercato.

Gli aggiornamenti dei sistemi antivirus utilizzati sono tempestivi ed effettuati più volte al giorno al fine di ottenere un accettabile standard di sicurezza delle banche dati trattati.

Nel caso in cui su uno o più sistemi si dovesse verificare perdita di informazioni o danni a causa di infezione o contagio da virus informatici l'amministratore di sistema deve provvedere a:

- isolare il sistema;
- verificare se ci sono altri sistemi infettati con lo stesso virus informatico;
- identificare l'antivirus adatto e bonificare il sistema infetto;
- installare l'antivirus adatto su tutti gli altri sistemi che ne sono sprovvisti.

13. FORMAZIONE DEL PERSONALE.

Il Titolare del trattamento dei dati personali valuta, per ogni persona cui hanno affidato un incarico o una responsabilità, sulla base dell'esperienza, delle sue conoscenze, ed in funzione anche di eventuali opportunità offerte dall'evoluzione tecnologica, se è necessario pianificare interventi di formazione.

La previsione di interventi formativi dei Soggetti Autorizzati al trattamento ha lo scopo principale di renderli edotti sui rischi che incombono sui dati, sulle misure disponibili per prevenire eventi dannosi, sui profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, sulle responsabilità che ne derivano e sulle modalità per aggiornarsi sulle misure minime adottate dal titolare.

La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali. La piena operatività del Regolamento UE 2016/679 dal 25/05/2018 impone di avviare un piano di formazione di tutto il personale.

In data 27 ottobre 2022 è stato realizzato l'intervento formativo programmato, sotto la docenza e responsabilità del DPO, Massimo Corinti, a cui hanno partecipato i seguenti soggetti:

vedi modello partecipanti

ELENCO PARTECIPANTI -corso

14. REGISTRO DELLE VIOLAZIONI DEI DATI PERSONALI (DATA BREACH).

14.1 Scopo del registro Data Breach.

Il presente documento contiene le indicazioni, le responsabilità e le azioni da attuare per la gestione della procedura da attivare in caso di possibile violazione dei dati personali, in osservanza agli obblighi relativi alla notifica all'Autorità Garante per la protezione dei dati personali e alla comunicazione all'interessato, in ossequio alle previsioni di cui agli articoli 33 e 34 del Regolamento Europeo 2016/679.

Tutti i soggetti (amministratori, dipendenti, collaboratori, ecc.) che trattano dati personali dell'Istituto devono essere informati e osservare la presente Procedura.

14.2 Organizzazione delle attività di gestione dell'evento violazione dei dati personali.

Il Titolare deve:

- designare un referente della gestione delle violazioni dei dati personali (di seguito referente data breach), figura che potrebbe coincidere con il Referente privacy dell'Ente.
- comunicare il nome del designato a tutti i soggetti autorizzati che trattano dati personali dell'Ente;
- avvalendosi del Referente data breach, predisporre il registro delle violazioni dei dati personali.

14.3 Gestione delle attività conseguenti ad una possibile violazione di dati personali.

Il soggetto che, a diverso titolo o in quanto autorizzato al trattamento di dati personali di cui è titolare l'Istituto, viene a conoscenza di una possibile violazione dei dati personali, deve immediatamente segnalare l'evento al Dirigente Scolastico e fornire la massima collaborazione.

La mancata segnalazione del suddetto evento comporta a diverso titolo responsabilità a carico del soggetto che ne è a conoscenza.

L'Istituto deve:

- adottare le Misure di sicurezza informatiche e/o organizzative per porre rimedio o attenuare i possibili effetti negativi della violazione dei dati personali e, contestualmente, informare immediatamente il Responsabile della Protezione dei Dati per una valutazione condivisa;

- condurre e documentare un'indagine corretta e imparziale sull'evento (aspetti organizzativi, informatici, legali, ecc.) attraverso la compilazione del "Modello di potenziale violazione di dati personali al Responsabile Protezione Dati";

- riferire i risultati dell'indagine inviando il modello al Responsabile della Protezione dei Dati.

Il Responsabile della Protezione dei Dati, ricevuti i risultati dell'indagine, analizza l'accaduto e formula un parere in merito all'evento, esprimendo la propria valutazione, non vincolante, che lo stesso configuri in una violazione dei dati personali e che possa comportare un probabile rischio per i diritti e le libertà delle persone fisiche e lo invia quindi al Dirigente Scolastico.

Il Dirigente Scolastico, tenuto conto del parere formulato dal Responsabile della Protezione dei Dati, se ritiene accertata la violazione dei dati personali e che la stessa possa comportare un probabile rischio per i diritti e le libertà delle persone fisiche, notifica tale violazione avvalendosi del "Modello comunicazione violazione all'Autorità Garante".

La notifica deve essere effettuata senza ingiustificato ritardo dall'accertamento dell'evento e, ove possibile, entro 72 ore dall'accertamento dello stesso con le modalità e i contenuti previsti dall'art. 33 del Regolamento Europeo 2016/679.

14.4 Comunicazione della violazione dei dati personali agli interessati.

Il Dirigente Scolastico, accertata la violazione dei dati personali e ritenendo che la stessa possa comportare un rischio elevato per i diritti e le libertà delle persone fisiche coinvolte, oltre alla notifica, decide le modalità di comunicazione di tale violazione agli interessati, come previsto dall'art. 34 del Regolamento Europeo 2016/679.

14.4 Compilazione del Registro delle violazioni dei dati personali.

Il Dirigente Scolastico documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nel Registro delle violazioni dei dati personali.

Tale documento è tenuto e implementato dal Titolare e consente all'autorità di controllo di verificare il rispetto dall'art. 33 del Regolamento Europeo 2016/679.

Per la redazione del registro è possibile ricorrere ad un file excel o al sistema di fascicolazione se disponibile nel programma di gestione documentale dell'Ente.

14.5 Registro delle violazioni dei dati personali (Data Breach) dell'Istituto Comprensivo "Tullio de Mauto" di Roma

Banca dati Violata	Data Violazione	Circostanze	Conseguenze della Violazione	Mitigazioni e/o Soluzioni	Data Comunicazione al Garante

15. MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE.

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, l'Istituto mette in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio.

L'Istituto è in procinto di adottare una serie di misure tecniche e organizzative atte a proteggere i dati personali e ad evitare che vi siano rischi per i diritti e le libertà delle persone fisiche.

MISURA ADOTTATA O ADOTTABILE	STATO	EVENTUALE DESCRIZIONE
Misure organizzative		
Determinazione dei termini di conservazione dei dati personali	Attiva	I dati sono conservati in cloud server Axios
Formazione di incaricati e responsabili	Attiva	
Privacy Policy	Attiva	
Accordi contrattuali con responsabili esterni	Attiva	
Verifica trasferimenti di dati personali al di fuori della UE	Attiva	I dati non vengono trasferiti extra UE
Analisi Privacy by Design e by Default della Modulistica	Attiva	
Valutazione dei rischi periodica	Da verificare	
Rispetto art.4 L. 300/1973 controllo dei lavoratori Regole per l'accesso alla posta elettronica in caso di assenza	Attiva	
Divieto di attività di controllo sistematico	Attiva	
Misure tecniche		
Verifica periodica delle misure di sicurezza adeguate al rischio	Da verificare	
Verifica periodica delle banche dati presenti (Data Discovery)	Attiva	
Procedure Data Breach	Attiva	
Procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento	Attiva	

Salvataggi dei dati personali	Da verificare	Sui server sono presenti backup sia giornalieri sia settimanali. I backup dei server salvano giornalmente i file critici, ad esclusione del sistema operativo.
Ripristino tempestivo della disponibilità e dell'accesso dei dati personali in caso di incidente fisico o tecnico	Attiva	Ci si basa sui report degli ultimi salvataggi fatti (sia per i backup globali sia per quelli parziali) e da lì si procede con i ripristini necessari e/o richiesti: · Ci si collega al server di backup che utilizza il prodotto Backup, avendo cura di utilizzare il file corretto · Avviare l'opzione di ripristino · Selezionare l'intera cartella o il singolo elemento da ripristinare alla data interessata · Attendere il ripristino di quanto richiesto
Permanenza di riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi di trattamento	Attiva	
Protezione da intrusioni esterne	Attiva	Firewall
Protezione da virus e malware	Attiva	Antivirus Microsoft e Firewall nella intranet
Protezione da accessi interni non autorizzati	Attiva	
Protezione delle reti wifi	Attiva	La rete wifi è comunque gestita con password
Aggiornamenti periodici dei software	Attiva	
Regole per la dismissione dell'hardware	Attiva	Prima di smaltire l'hardware presso uno smaltitore accreditato, si provvede a rendere illeggibili i dati contenuti nei dischi.
Protezione da interruzioni di energia elettrica	Attiva	E' presente 1 gruppi di continuità. La durata della continuità fornita è di circa 30 minuti. Le postazioni di lavoro non sono sotto gruppo.
Verifica della sicurezza sito internet	Attiva	
Cifratura dei dati	Attiva	Server AXIOS
Protezione delle postazioni di lavoro da accessi	Attiva	
Protezione da installazioni di software non autorizzato	Attiva	
Sicurezza delle credenziali di accesso	Attiva	
Controllo accessi al sistema informativo	Attiva	
Protezione del sito internet da minacce hacker	Attiva	
Controllo antivirus in invio e ricezione posta	Attiva	
Adozione di crittografia in trasmissione di dati	Attiva	
Protezione dei log di navigazione internet	Attiva	

Cancellazione periodica dei log di navigazione	Attiva	

16. GESTIONE DEI DIRITTI DEGLI INTERESSATI.

Come previsto dall'art. 12 par. 3, 4 e 5 del GDPR, in caso di richiesta di uno o più interessati di avvalersi dei propri diritti, ai sensi degli art. 15-22 del GDPR, con invio di richiesta scritta e circostanziata ai dati di contatto del Responsabile della Protezione dei dati personali, l'Istituto avvia immediatamente le operazioni necessarie a soddisfare tale richiesta.

L'Istituto provvede nei tempi previsti dal Regolamento, quindi al massimo entro un mese, ad inviare un riscontro, sia positivo che negativo, all'interessato che ha formulato la richiesta, mediante posta elettronica, salvo diversa indicazione dell'interessato.

Dopodiché registra l'evento nella tabella sottostante, al fine di tenere traccia di tutte le eventuali richieste e se le stesse sono manifestamente infondate o eccessive, in particolare per il loro carattere ripetitivo, il titolare del trattamento può:

a) addebitare un contributo spese ragionevole tenendo conto dei costi amministrativi sostenuti per fornire le informazioni o la comunicazione o intraprendere l'azione richiesta;

b) rifiutare di soddisfare la richiesta.

Data Richiesta	Natura della Richiesta	Interessato	Azione intrapresa	Data risposta all'interessato

17. PRIVACY POLICY

A tutti i soggetti autorizzati è stata consegnata, in formato cartaceo o in .pdf, la Privacy Policy dell'Istituto, che viene riportata in Allegato 1 nella sua ultima versione.

18. ADESIONE AI CODICI DI CONDOTTA

Il titolare aderisce al codice di condotta dei dipendenti pubblici (si veda l'albo dell'Istituto).

19. REVISIONE

La presente versione V1 del Registro è datata 04 ottobre 2022, è relativa alla prima stesura.

ALLEGATO 1: PRIVACY POLICY

PRIVACY POLICY

dell'Istituto per l'utilizzo degli strumenti di lavoro

Indice

Premessa

La progressiva diffusione delle nuove tecnologie informatiche e, in particolare, il libero accesso alla rete Internet dai Personal Computer, Tablet, Smartphone e più in generale ogni apparato in grado di connettersi alla rete, espone l'Istituto e gli utenti (dipendenti e collaboratori della stessa) a rischi di natura patrimoniale, oltre alle responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge (legislazione sul diritto d'autore e sulla privacy, fra tutte), creando evidenti problemi alla sicurezza ed all'immagine dell'Istituto stesso.

Premesso quindi che l'utilizzo degli strumenti di lavoro, nei quali sono compresi anche i sistemi e le risorse informatiche e telematiche, deve sempre ispirarsi al principio della diligenza e correttezza, propri del rapporto di lavoro, **l'Istituto adotta la presente Privacy Policy** diretta ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla Sicurezza nel trattamento dei dati nonché originare responsabilità in capo all'Istituto ovvero ai singoli lavoratori.

Le prescrizioni di seguito previste si aggiungono ed integrano le specifiche istruzioni fornite a tutti i soggetti autorizzati in attuazione del Regolamento 2016/679/UE (nel seguito "GDPR") e del D.lgs. 30 giugno 2003 n. 196 (di seguito "Codice") come modificato dal D.lgs. 101/2018, relativamente alle prescrizioni non in contrasto con il GDPR, nonché integrano le informazioni fornite agli interessati in ordine alle ragioni e alle modalità dei possibili controlli o alle conseguenze di tipo disciplinare in caso di violazione delle stesse. Si tiene conto, purchè non in contrasto con il GDPR, delle principali prescrizioni e le linee guida del Garante privacy in relazione al trattamento di dati personali effettuato ai fini delle verifiche per il corretto utilizzo della posta elettronica e della rete Internet da parte dei dipendenti (provvedimento del 1° marzo 2007) nonché delle previsioni dell'art. 4 l. 300/70, come modificato dal D.lgs.. 151/2015 relativamente ai controlli sugli "strumenti di lavoro", e tenendo presente le indicazioni fornite dal WP 29 con la "Opinion 2/2017 on data processing at work".

Dal contesto tracciato dal Garante nelle premesse dei citati provvedimenti emerge che:

- compete ai datori di lavoro assicurare la funzionalità e il corretto impiego di tali mezzi da parte dei lavoratori, definendone le modalità d'uso nell'organizzazione dell'attività lavorativa, tenendo conto della disciplina in tema di diritti e relazioni sindacali;
- spetta sempre ai datori di lavoro adottare idonee misure di sicurezza per assicurare la disponibilità e l'integrità di sistemi informativi e dei dati, anche per prevenire utilizzi indebiti che possono essere fonte di responsabilità;
- è necessario tutelare i lavoratori interessati anche perché l'utilizzazione dei predetti mezzi, già ampiamente diffusi nel contesto lavorativo, è destinata ad un rapido incremento in numerose attività svolte anche fuori della sede lavorativa;
- l'utilizzo di Internet da parte dei lavoratori può infatti formare oggetto di analisi, profilazione e integrale ricostruzione mediante elaborazione di file di log, della navigazione web ottenuti, ad esempio, da un proxy server o da un altro strumento di registrazione delle informazioni. I servizi di posta elettronica sono parimenti suscettibili (anche attraverso la tenuta dei file di

log di traffico e-mail e l'archiviazione di messaggi) di controlli che possono giungere fino alla conoscenza da parte del datore di lavoro (titolare del trattamento) del contenuto della corrispondenza;
- le informazioni così trattate contengono dati personali anche sensibili riguardanti lavoratori o terzi, identificati o identificabili.

Alla luce delle premesse sopra riportate ed avendo in considerazione che l'Istituto nell'ottica di uno svolgimento proficuo e più agevole della propria attività, ha da tempo deciso di mettere a disposizione dei propri collaboratori che ne necessitassero per il tipo di funzioni svolte, telefoni e mezzi di comunicazione efficienti (computer desk-top e/o portatili, telefoni cellulari, etc.), sono state inserite in questo documento le opportune indicazioni ed istruzioni relative alle modalità ed ai doveri che ciascun lavoratore deve osservare nell'utilizzo di tale strumentazione.

1. Entrata in vigore del regolamento e pubblicità

1.1 Con l'entrata in vigore del presente Privacy Policy tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalle presenti.

1.2 Copia di questo documento viene pubblicato sul sito istituzionale dell'Istituto, ed allegato alla comunicazione che ne ufficializza l'adozione nelle forme e con le modalità in uso presso l'Istituto.

2. Campo di applicazione

2.1 La Privacy Policy si applica a tutti i lavoratori, ossia ai dipendenti, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori dell'Istituto a prescindere dal rapporto contrattuale con la stessa intrattenuto.

2.2 Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "utente" deve intendersi ogni lavoratore in possesso di specifiche credenziali di autenticazione. Tale figura sarà anche indicata quale "Soggetto Autorizzato al trattamento" nell'accezione propria dell'art. 29 del GDPR.

3. Utilizzo del Personal Computer

3.1 **Il Personal Computer affidato all'utente è uno strumento di lavoro**. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Il personal computer (PC) deve essere custodito con cura evitando ogni possibile forma di danneggiamento.

3.2 Il personal computer dato in affidamento all'utente permette l'accesso alla rete solo attraverso specifiche **credenziali di autenticazione** come meglio descritto al successivo punto 4 del presente documento.

3.3 Il personale nominato "soggetto autorizzato", per l'espletamento delle sue funzioni e per garantire la sicurezza del sistema informatico, ha la facoltà, in qualunque momento, di accedere ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica, come più specificatamente precisato al successivo punto 13.1 del presente documento. La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività dell'Istituto, si applica anche in caso di assenza prolungata od impedimento dell'utente. Analoghe verifiche possono essere effettuate sui siti internet acceduti dagli utenti abilitati alla navigazione esterna. L'accesso, comunque, verrà effettuato con modalità tali da evitare qualsiasi forma di controllo a distanza. In ogni caso, l'Istituto garantisce la non effettuazione di alcun trattamento mediante sistemi *hardware* e *software* specificatamente preordinati al controllo a distanza, quali, a titolo esemplificativo:
   - lettura e registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio *e-mail*;
   - riproduzione ed eventuale memorizzazione sistematica delle pagine *web* visualizzate dal lavoratore;
   - la lettura e la registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;
   - l'analisi occulta di computer portatili affidati in uso.

3.4 Non è consentito l'uso di programmi diversi da quelli ufficialmente installati né viene consentito agli utenti di installare autonomamente programmi provenienti dall'esterno, sussistendo infatti il grave pericolo di introdurre Virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti. L'inosservanza della presente disposizione espone lo stesso Istituto a gravi responsabilità civili; si evidenzia inoltre che le violazioni della normativa a tutela dei diritti d'autore sul software che impone la presenza nel sistema di software regolarmente licenziato, o comunque libero e quindi non protetto dal diritto d'autore, vengono sanzionate anche penalmente.

3.6 Salvo preventiva espressa autorizzazione del Delegato Interno al trattamento, non è consentito all'utente modificare le caratteristiche impostate sul proprio PC né procedere ad installare dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, etc.).

3.7 Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il Delegato Interno al trattamento nel caso in cui siano rilevati virus e adottando quanto previsto dal successivo punto 10 del presente Regolamento relativo alle procedure di protezione antivirus.

3.8 Il Personal Computer deve essere spento prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio o in caso di suo inutilizzo. In ogni caso, lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso. Al fine di evitare tali evenienze si dovrà "bloccare" l'utilizzo del PC prima di allontanarsi o impostare la modalità "screen saver" che prevede la richiesta della password per riattivarne l'uso**.**

4. Gestione ed assegnazione delle credenziali di autenticazione

4.1 Le credenziali di autenticazione per l'accesso alla rete vengono assegnate dal Delegato Interno al trattamento, previa formale richiesta.

4.2 Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (user id), associato ad una parola chiave (password) riservata che dovrà venir custodita dal Soggetto Autorizzato con la massima diligenza e non divulgata. Non è consentita l'attivazione della password di accensione (bios), senza preventiva autorizzazione da parte del Delegato Interno al trattamento.

4.3 La parola chiave, formata da lettere (maiuscole o minuscole) e/o numeri, anche in combinazione fra loro, deve essere composta da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili al Soggetto Autorizzato. Per costruire la password utilizzare:
   - lettere, numeri e almeno un carattere tra . ; $! @ - > <
   - Non utilizzare date di nascita, nomi o cognomi propri o di parenti

- Non sceglierla uguale alla matricola o alla userid
- Custodirla sempre in un luogo sicuro e non accessibile a terzi
- Non divulgarla a terzi e non condividerla con altri utenti

4.4 È necessario procedere alla modifica della parola chiave a cura dell'utente, ove ciò non avvenga grazie a processi automatici del sistema informativo, al primo utilizzo e, successivamente, almeno ogni sei mesi (Ogni tre mesi nel caso invece di trattamento di dati sensibili attraverso l'ausilio di strumenti elettronici).

4.5 Qualora la parola chiave dovesse venir sostituita, per decorso del termine sopra previsto e/o in quanto abbia perduto la propria riservatezza, si procederà in tal senso d'intesa con il Delegato Interno al trattamento.

5. Utilizzo della rete interna

5.1 Per l'accesso alla rete dell'Istituto ciascun utente deve essere in possesso della specifica credenziale di autenticazione.

5.2 È assolutamente proibito entrare nella rete e nei programmi con un codice d'identificazione utente diverso da quello assegnato. Le parole chiave d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le istruzioni impartite.

5.3 Le cartelle utenti presenti nei server dell'Istituto sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto, qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità vengono svolte regolari attività di controllo, amministrazione e back up da parte del Delegato Interno al trattamento. Si ricorda che tutti i dischi o altre unità di memorizzazione locali (es. disco C: interno PC) non sono soggette a salvataggio da parte del personale nominato Soggetto Autorizzato. La responsabilità del salvataggio dei dati ivi contenuti è pertanto a carico del singolo utente.

5.4 Il Delegato Interno al trattamento può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza sia sui PC dei Soggetti Autorizzati sia sulle unità di rete.

5.5 Risulta opportuno che, con regolare periodicità (almeno ogni tre mesi), ciascun utente provveda alla pulizia degli archivi del proprio PC, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.

6. Utilizzo e conservazione dei supporti rimovibili

6.1 Tutti i supporti magnetici rimovibili (CD e DVD riscrivibili, supporti USB, hard-disk removibili, ecc.), contenenti dati rilevanti, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato.

6.2 Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati sensibili, ciascun utente dovrà contattare il Delegato Interno al trattamento e seguire le istruzioni da questo impartite.

6.3 In ogni caso, i supporti magnetici contenenti dati **particolari/sensibili**, secondo la definizione dell'art. 4 del GDPR, devono essere adeguatamente custoditi dagli utenti e risposti in armadi chiusi ad accesso controllato.

6.4 È vietato l'utilizzo di supporti rimovibili personali.

6.5 L'utente è responsabile della custodia dei supporti e dei dati personali in essi contenuti.

7. Utilizzo di PC portatili

7.1 L'utente è responsabile del PC portatile assegnatogli dal Delegato Interno al trattamento e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

7.2 Ai PC portatili si applicano le regole di utilizzo previste per i PC desktop.

7.3 I PC portatili utilizzati all'esterno, in caso di allontanamento, devono essere custoditi con diligenza, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni.

8. Uso della posta elettronica

8.1 **La casella di posta elettronica assegnata all'utente è uno strumento di lavoro.** Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

8.2 È fatto divieto di utilizzare le caselle di posta elettronica istituzionali per motivi diversi da quelli strettamente legati all'attività lavorativa. In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare la posta elettronica per:

- l'invio e/o il ricevimento di allegati contenenti filmati o brani musicali (es.mp3) non legati all'attività lavorativa;
- l'invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list;
- la partecipazione a catene telematiche. Se si dovessero peraltro ricevere messaggi di tale tipo, comunicarlo immediatamente al Delegato Interno al trattamento. Non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi.

8.3 La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili.

8.4 Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per l'Istituto ovvero contenga documenti da considerarsi riservati, deve essere preventivamente visionata od autorizzata dal Delegato Interno al trattamento.

8.5 È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario. Si evidenzia però che le comunicazioni ufficiali, da inviarsi mediante gli strumenti tradizionali, possono richiedere l'autorizzazione e la firma dei Responsabili di ufficio, a seconda del loro contenuto e dei destinatari delle stesse.

8.6 È obbligatorio controllare i file attachment di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

8.7 Al fine di ribadire agli interlocutori la natura esclusivamente istituzionale della casella di posta elettronica, i messaggi devono contenere un avvertimento standardizzato nel quale sia dichiarata la natura non personale dei messaggi stessi precisando che, pertanto, personale dipendente dell'Istituto debitamente nominato Soggetto Autorizzato potrà accedere al contenuto del messaggio inviato alla stessa casella secondo le regole fissate nel presente documento. Si riportano di seguito i testi da utilizzare:

Le informazioni contenute nella presente e-mail potrebbero essere confidenziali e sono dirette unicamente ai destinatari sopra indicati. In caso di ricezione da parte di persona diversa è vietato qualunque tipo di distribuzione o copia. Chi riceva questo messaggio per errore è pregato di inoltrarlo al mittente e di distruggere questa e-mail.

8.8 Come anticipato al precedente punto 3.3 del presente documento, il personale nominato Soggetto Autorizzato potrà accedere ai dati contenuti nelle caselle di posta elettronica di lavoro per le sole finalità ivi indicate.

9. Navigazione in Internet

9.1. **Il PC assegnato al singolo utente ed abilitato alla navigazione in Internet costituisce uno strumento istituzionale utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa**. È quindi assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa.

9.2 In questo senso, a titolo puramente esemplificativo, **l'utente non potrà utilizzare Internet** per:

- l'upload o il download di software gratuiti (freeware) e shareware, nonché l'utilizzo di documenti provenienti da siti web o http, se non strettamente attinenti all'attività lavorativa (filmati e musica) e previa verifica dell'attendibilità dei siti in questione (nel caso di dubbio, dovrà venir a tal fine contattato il Delegato Interno al trattamento);
- l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, fatti salvi i casi direttamente autorizzati dall'Istituto (o eventualmente dal Delegato Interno al trattamento) e comunque nel rispetto delle normali procedure di acquisto;
- ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa;
- la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames) se non espressamente autorizzati dal Delegato Interno al trattamento;
- l'accesso, tramite Internet, a caselle webmail di posta elettronica personale, salvo specifica autorizzazione.

9.3 Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, l'Istituto può prevedere l'adozione di uno specifico sistema di blocco o filtro automatico che prevengano determinate operazioni quali l'upload o l'accesso a specificati siti inseriti in una black list.

9.4 In conformità al punto 3.3, il personale nominato Soggetto Autorizzato potrà procedere a controlli sulla navigazione finalizzati esclusivamente a garantire l'operatività e la sicurezza del sistema, nonché il necessario svolgimento delle attività lavorative, es. mediante un sistema di controllo dei contenuti (Proxy server) o mediante "file di log" della navigazione svolta. Il controllo sui file di log non è continuativo ed i file stessi vengono conservati non oltre 6 mesi.

10. Protezione antivirus

10.1 Il sistema informatico dell'Istituto è protetto da software antivirus aggiornato periodicamente. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico istituzionale mediante virus o mediante ogni altro software aggressivo.

10.2 Nel caso il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer nonché segnalare prontamente l'accaduto al Delegato Interno al trattamento.

10.3 Ogni dispositivo magnetico di provenienza esterna all'Istituto dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere prontamente consegnato al Delegato Interno al trattamento.

11. Utilizzo dei telefoni e fotocopiatrici dell'Istituto.

11.1 L'eventuale telefono affidato al lavoratore è uno strumento di lavoro. Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa, non essendo quindi consentite comunicazioni a carattere personale o comunque non strettamente inerenti all'attività lavorativa stessa. La ricezione o l'effettuazione di telefonate personali è consentita sempre che vengano rispettati i criteri di ragionevolezza ovvero nel caso di necessità ed urgenza.

11.2 Qualora venisse assegnato un cellulare (o smartphone, tablet, etc.) istituzionale all'utente, quest'ultimo sarà responsabile del suo utilizzo e della sua custodia. Al cellulare istituzionale si applicano le medesime regole sopra previste per l'utilizzo del telefono istituzionale: in particolare è vietato l'utilizzo del telefono cellulare messo a disposizione per inviare o ricevere SMS di natura personale o comunque non pertinenti rispetto allo svolgimento dell'attività lavorativa. L'eventuale uso promiscuo (anche per fini personali) del telefono cellulare istituzionale è possibile soltanto in presenza di preventiva autorizzazione scritta e in conformità delle istruzioni al riguardo impartite dall'Istituto.

11.3 È vietato l'utilizzo delle fotocopiatrici per fini personali, salvo preventiva ed esplicita autorizzazione da parte del Delegato Interno al trattamento.

12. Osservanza delle disposizioni in materia di Privacy

12.1 È obbligatorio attenersi alle disposizioni in materia di protezione dei dati personali previste dal GDPR, e dal Codice, rispettando le misure di sicurezza adottate dall'Istituto, nonché le istruzioni fornite con la designazione a "Soggetto Autorizzato al trattamento dei dati", come previsto dall'art. 29 del GDPR, applicando puntualmente le disposizioni ivi contenute nonché ogni ulteriore indicazione comunicata, anche per le vie brevi, dal Delegato Interno al trattamento.

12.2 I "Soggetti Autorizzati" che sono addetti alle attività di amministrazione e gestione dei Sistemi, Data Base e della Infrastruttura di connessione dovranno rispettare le specifiche istruzioni loro fornite al fine di rispettare i principi di necessità e di legittimità e correttezza nella effettuazione delle loro attività. I nominativi di coloro che hanno competenza sui sistemi che trattano dati personali dei dipendenti dell'Istituto potranno essere comunicati nelle modalità e con le forme previste dalla normativa applicabile.

13. Accesso ai dati trattati dall'utente

13.1 Oltre che per motivi di sicurezza del sistema informatico, anche per motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.) comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è facoltà dell'Istituto, accedere direttamente, nel rispetto della normativa sulla privacy, a tutti gli strumenti informatici istituzionali e ai documenti ivi contenuti, nonché ai tabulati del traffico telefonico.

14. Gestione Archivi cartacei

14.1 Quando si tratta di applicare e adottare il GDPR, per i documenti cartacei come per qualsiasi informazione personale detenuta, i soggetti autorizzati dell'Istituto devono esaminare le modalità di archiviazione delle informazioni e agire secondo le seguenti regole.

14.2 Stampare semplicemente un documento e dimenticarsi di averlo fatto può costituire un rischio per la sicurezza e bisogna considerare che dei soggetti non autorizzati potrebbero accidentalmente prendere quel documento stampato.
Ogni volta che si invia un documento da stampare tramite una stampante wireless o di rete, si corre il rischio di violazioni della sicurezza.

14.3. I documenti cartacei da conservare devono essere gestiti in modo da poter essere rintracciati e individuati facilmente. I documenti cartacei contenenti dati particolari sensibili o giudiziari devono essere conservati in armadietti chiusi a chiave il cui accesso è limitato soltanto alle persone autorizzate a quel trattamento all'interno dell'Istituto.

14.4. Lo smaltimento sicuro della carta deve essere una priorità, in particolare ora che l'UE ha aumentato le sue richieste in materia di protezione dei dati. I documenti cartacei non più necessari devono essere smaltiti in modo conforme. Bisogna utilizzare la macchina distruggidocumenti o in mancanza agire manualmente spezzettando i fogli in piccole parti in modo da non essere più ricomponibili.

14.5 I documenti cartacei contenenti dati personali devono essere custoditi in modo da non essere accessibili a persone non autorizzate al trattamento (es. armadi o cassetti chiusi a chiave).

I documenti cartacei che vengono prelevati dagli archivi per l'attività quotidiana devono esservi riposti nel periodo di intervallo meridiano e a fine giornata e non devono rimanere incustoditi su scrivanie o tavoli di lavoro.

14.6 I documenti cartacei contenenti dati particolari sensibili o giudiziari devono essere controllati e custoditi dai soggetti autorizzati in modo che non vi possano accedere persone prive di autorizzazione. La loro consultazione deve avvenire per il tempo strettamente necessario alla necessità di utilizzo e, subito dopo, i documenti devono essere nuovamente archiviati.

14.7 La presenza di ospiti o di personale non autorizzato non è consentita in luoghi in cui siano presenti documenti cartacei in vista.

14.8 Evitare assolutamente di prendere appunti su fogli di carta accumulati per il riciclo senza badare a ciò che è stampato sul retro: tipicamente si tratta di vecchi documenti stampati che possono contenere dati personali e particolari sensibili o giudiziari.

15. Sistemi di controlli graduali

15.1 In caso di anomalie e su mandato dell'Istituto, il personale nominato Soggetto Autorizzato del trattamento o gli addetti alla manutenzione, effettuerà controlli anonimi che si concluderanno con avvisi generalizzati diretti ai dipendenti dell'area o del settore in cui è stata rilevata l'anomalia, nei quali si evidenzierà l'utilizzo irregolare degli strumenti istituzionali e si inviteranno gli utenti ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite. Controlli su base individuale potranno essere computi solo in caso di successive ulteriori anomalie.

15.2. In alcun caso verranno compiuti controlli prolungati, costanti o indiscriminati.

16. Sanzioni

16.1 È fatto obbligo a tutti i lavoratori di osservare le disposizioni portate a conoscenza con il presente documento. Il mancato rispetto o la violazione delle regole sopra ricordate possono di per sé considerarsi contrari ai doveri di diligenza e fedeltà previsti dagli artt. 2104 e 2105 del Codice civile e sono perseguibili nei confronti del personale dipendente con provvedimenti disciplinari e risarcitori previsti dal Contratto di lavoro sottoscritto ovvero dal vigente CCNL, nonché con tutte le azioni civili e penali consentite.

17. Aggiornamento e revisione

17.1 Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni motivate al presente documento. Le proposte verranno esaminate dall'Istituto.

17.2 Il presente documento è soggetto a revisione con frequenza periodica anche in funzione dell'introduzione di nuovi strumenti di lavoro e/o informatici, dell'evoluzione tecnologica o di cambiamenti normativi.

ALLEGATO 2: MODELLO SEGNALAZIONE DATA BREACH PA.

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

VIOLAZIONE DI DATI PERSONALI

Secondo quanto prescritto dal **Provvedimento del 2 luglio 2015**, le amministrazioni pubbliche sono tenute a comunicare al Garante all'indirizzo: **databreach.pa@pec.gpdp.it** le violazioni dei dati personali (*data breach*) che si verificano nell'ambito delle banche dati (qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti, art. 4, comma 1, lett. *p* del Codice) di cui sono titolari.

La comunicazione deve essere effettuata entro 48 ore dalla conoscenza del fatto, compilando il modulo che segue.

Istituto Titolare del trattamento

Denominazione: _____

Provincia: _____ Comune:_____ Cap :_____

Indirizzo: _____

Nome persona fisica addetta alla comunicazione:_____

Cognome persona fisica addetta alla comunicazione:_____

Funzione rivestita:_____

Indirizzo PEC e/o EMAIL per eventuali comunicazioni:_____

Recapito telefonico per eventuali comunicazioni: _____

Eventuali Contatti (altre informazioni):_____

Denominazione della/e banca/banche dati oggetto di data breach e breve descrizione della violazione dei dati personali ivi trattati:

Quando si è verificata la violazione dei dati personali trattati nell'ambito della banca dati?

- ☐ Il _____
- ☐ Tra il _____ e il _____
- ☐ In un tempo non ancora determinato
- ☐ E' possibile che sia ancora in corso

Dove è avvenuta la violazione dei dati? (Specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili)

Modalità di esposizione al rischio

Tipo di violazione

- ☐ Lettura (presumibilmente i dati non sono stati copiati)
- ☐ Copia (i dati sono ancora presenti sui sistemi del titolare)
- ☐ Alterazione (i dati sono presenti sui sistemi ma sono stati alterati)
- ☐ Cancellazione (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione)
- ☐ Furto (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione)
- ☐ Altro : _____

Dispositivo oggetto della violazione

- ☐ Computer
- ☐ Rete
- ☐ Dispositivo mobile
- ☐ File o parte di un file Strumento di *backup*
- ☐ Documento cartaceo
- ☐ Altro : _____

Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione:

Quante persone sono state colpite dalla violazione dei dati personali trattati nell'ambito della banca dati?

- ☐ N. _____ persone
- ☐ Circa _____ persone
- ☐ Un numero (ancora) sconosciuto di persone

Che tipo di dati sono oggetto di violazione?

- ☐ Dati anagrafici/codice fiscale
- ☐ Dati di accesso e di identificazione (*user name*, *password*, *customer ID*, altro)
- ☐ Dati relativi a minori

- ☐ 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
- ☐ Dati personali idonei a rivelare lo stato di salute e la vita sessuale
- ☐ Dati giudiziari
- ☐ Copia per immagine su supporto informatico di documenti analogici
- ☐ Ancora sconosciuto
- ☐ Altro : _____

Livello di gravità della violazione dei dati personali trattati nell'ambito della banca dati (secondo le valutazioni del titolare)?

- ☐ Basso/trascurabile
- ☐ Medio
- ☐ Alto
- ☐ Molto alto

Misure tecniche e organizzative applicate ai dati oggetto di violazione

La violazione è stata comunicata anche agli interessati?

- ☐ Sì, è stata comunicata il _____
- ☐ No, perché _____

Qual è il contenuto della comunicazione resa agli interessati?

Quali misure tecnologiche e organizzative sono state assunte per contenere la violazione dei dati e prevenire simili violazioni future?

ALLEGATO 3: NOMINA A DELEGATO INTERNO AL TRATTAMENTO DEI DATI PERSONALI.

NOMINA A DELEGATO INTERNO AL TRATTAMENTO DEI DATI PERSONALI

Al Direttore dei Servizi Generali e Amministrativi

Oggetto: Nomina a Delegato Interno del Trattamento dati personali

L'Istituto Comprensivo Statale "Tullio De Mauro", con codice fiscale 97567160581, in qualità di Titolare del trattamento dei dati personali nella persona del Dirigente Scolastico Dott.ssa Patrizia Tozi:

VISTO il Regolamento UE 2016/679 con particolare riguardo agli artt. 24, 28, 29 e 32;

VISTO il Decreto Legislativo 30 giugno 2003, n. 196, "Codice in materia di protezione dei dati personali", nel seguito indicato sinteticamente come Codice, e successive modificazioni e integrazioni (in particolare il Decreto Legislativo 101/2018,

CONSIDERATO che questo Istituto è Titolare del trattamento dei dati personali di alunni, genitori, personale dipendente, fornitori, e qualunque altro soggetto che abbia rapporti con l'Istituto medesimo e che a questo conferisca, volontariamente o per obbligo, propri dati personali;

CONSIDERATO che la titolarità del trattamento dei dati personali è esercitata dallo scrivente Dirigente dell'Istituto, in qualità di legale rappresentante dello stesso;

CONSIDERATO che la S.V., in servizio presso questo Istituto come Direttore dei Servizi Generali ed Amministrativi, per profilo professionale, funzione rivestita, esperienza, capacità ed affidabilità fornisce idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati personali, ivi compreso il profilo relativo alla sicurezza;

VISTO il CCNL vigente e il relativo profilo professionale del DSGA

DESIGNA

___xxxxxxx_____ quale Delegato Interno del trattamento dei dati personali, in relazione alle operazioni di elaborazione di dati personali, su supporto cartaceo e/o digitale, alle quali il personale sottoposto alla Sua direzione, controllo e coordinamento, ha accesso nell'espletamento delle funzioni e dei compiti assegnati nell'ambito del rapporto di lavoro con questa istituzione scolastica e disciplinati dalla normativa in vigore e dai contratti di settore.

COMPITI E AMBITI

La S.V. svolgerà i Suoi compiti e sovrintenderà alle operazioni relative al trattamento, attenendosi alle seguenti istruzioni generali:

1. operare e vigilare, in collaborazione con la scrivente, affinché il trattamento dei dati personali avvenga secondo le modalità definite dalla normativa più sopra indicata e delle prassi amministrative correlate, fino a che il presente incarico non venga revocato o non cessi il rapporto di lavoro con l'istituzione scolastica;
2. operare in relazione ai trattamenti effettuati dall'Istituzione scolastica, trattare i dati personali nell'ambito delle finalità istituzionali della scuola, che sono quelle relative all'istruzione ed alla formazione degli alunni e quelle amministrative ad esse strumentali, così come definite dalla normativa vigente;
3. riportare alla scrivente le problematiche di maggior rilievo nell'ambito del trattamento dei dati personali, al fine di una sua decisione in merito;
4. adottare, d'intesa con la scrivente, tutte le misure atte a garantire l'esattezza, l'aggiornamento e la pertinenza dei dati personali trattati dall'Istituto, nonché garantire esercizio dei diritti degli interessati,
5. verificare che agli interessati venga effettivamente fornita le Informazioni ex art. 13 del Regolamento;

6. non ricorrere a Responsabili del Trattamento, a meno che non ci sia una espressa autorizzazione scritta del Titolare;
7. collaborare con la scrivente nella predisposizione, nell'adozione e nell'aggiornamento periodico delle misure di sicurezza previste dall'art. 32 del Regolamento, con riguardo anche all'attuazione della Direttiva 1 agosto 2015 del Presidente del Consiglio dei Ministri (elenco ufficiale delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni), della Circolare 18 aprile 2017, n. 2/2017 e dei futuri aggiornamenti di questi atti;
8. collaborare con la scrivente per la predisposizione di attività formative per le persone autorizzate al trattamento dei dati personali che abbiano ricevuto le istruzioni di cui agli articoli 29 e 32 del Regolamento;
9. provvedere affinché siano consegnati, all'atto dell'assunzione in servizio, a tutto il personale - anche temporaneo - di questa istituzione scolastica gli atti di incarico, con autorizzazione al trattamento e istruzioni, sia individuali che collettivi e gli eventuali documenti a questi allegati, controllando il rispetto dei correlati obblighi di riservatezza;
10. contribuire alle attività di revisione delle misure organizzative e alle ispezioni poste in essere dal Titolare e informare il Titolare qualora una istruzione data violi il Regolamento e la normativa correlata;
11. attivare immediatamente la procedura di disattivazione delle password smarrite e/o rubate e di attribuzione ai Soggetti Autorizzati di nuove credenziali di accesso ogni qualvolta venga comunicata o accertata una fattispecie di smarrimento o furto di credenziali di autenticazione ai computer (codice di accesso e parola chiave);
12. disporre la disattivazione ogni qualvolta venga comunicato o accertato il caso in cui le credenziali di autenticazione non vengano utilizzate per almeno sei mesi;
13. adottare le idonee misure organizzative per fronteggiare i casi di assenza o impedimento di Soggetti Autorizzati al trattamento.

In particolare, in qualità di addetti ai servizi amministrativi e generali della scuola, sia la S.V. che il personale sottoposto alla Sua direzione, controllo e coordinamento, sono incaricate delle operazioni di raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, modifica, comunicazione (nei soli casi autorizzati dal Titolare o dal Delegato Interno al trattamento), selezione, estrazione di dati, connesse alle seguenti funzioni e attività esercitate:

Alunni e genitori
- gestione archivi elettronici alunni e genitori;
- gestione archivi cartacei con fascicoli personali alunni;
- consultazione documenti e registri di attestazione dei voti e di documentazione della vita scolastica dello studente, nonché delle relazioni tra scuola e famiglia quali ad esempio richieste, istanze e corrispondenza con le famiglie;
- gestione contributi e/o tasse scolastiche versati da alunni e genitori;
- adempimenti connessi alla corretta gestione del Registro infortuni;
- adempimenti connessi a Viaggi di istruzione, visite guidate e uscite didattiche.

Personale ATA e Docenti
- gestione archivi elettronici Personale ATA e Docenti;
- gestione archivi cartacei Personale ATA e Docenti;
- tenuta documenti e registri relativi alla vita lavorativa dei dipendenti (quali ad es. assenze, convocazioni, comunicazioni, documentazione sullo stato del personale, atti di nomina del personale a tempo determinato, decreti del Dirigente).

Contabilità e finanza
- gestione archivi elettronici della contabilità;
- gestione stipendi e pagamenti, nonché adempimenti di carattere previdenziale;
- gestione documentazione ore di servizio (quali ad esempio, registrazione delle ore eccedenti);

- gestione rapporti con i fornitori;
- gestione Programma annuale e fondo di istituto;
- corretta tenuta dei registri contabili previsti dal Decreto interministeriale n. 44/2001 e correlata normativa vigente.

Protocollo e archivio corrispondenza ordinaria
- attività di protocollo e archiviazione della corrispondenza ordinaria.

Attività organi collegiali
- eventuale operazione di consultazione e estrazione dati dai verbali degli organi collegiali.

ISTRUZIONI OPERATIVE

Si rende noto, a tal fine, che le operazioni sopra descritte vanno rigorosamente effettuate tenendo presenti le istruzioni operative che seguono:

1. il trattamento dei dati personali a cui la S.V. e il personale sottoposto alla Sua direzione, controllo e coordinamento sono autorizzate ad accedere deve avvenire secondo le modalità definite dalla normativa in vigore, in modo lecito e secondo correttezza e con l'osservanza - in particolare - delle prescrizioni di cui al Regolamento UE 2016/679 e al d.lgs. 196/2003 e s.m.i.;
2. il trattamento dei dati personali è consentito soltanto per lo svolgimento delle funzioni istituzionali della scuola;
3. i dati personali, oggetto dei trattamenti, devono essere esatti ed aggiornati, inoltre devono essere pertinenti, completi e non eccedenti le finalità per le quali vengono raccolti e trattati;
4. è vietata qualsiasi forma di diffusione e comunicazione dei dati personali trattati che non sia strettamente funzionale allo svolgimento dei compiti affidati e autorizzata dal Delegato Interno o dal Titolare del trattamento. Si raccomanda particolare attenzione alla tutela del diritto alla riservatezza degli interessati (persone fisiche a cui afferiscono i dati personali);
5. mantenere la dovuta riservatezza in ordine alle informazioni delle quali si sia venuti a conoscenza nel corso dell'incarico; tale obbligo deve permanere in ogni caso, anche quando sia venuto meno l'incarico stesso;
6. i trattamenti andranno effettuati rispettando le misure di sicurezza predisposte nell'istituzione scolastica; in ogni operazione di trattamento andrà garantita la massima riservatezza e custodia degli atti e dei documenti contenenti dati personali che non andranno mai lasciati incustoditi o a disposizione di terzi non autorizzati ad accedervi, prendervi visione o ad effettuare qualsivoglia trattamento;
7. le eventuali credenziali di autenticazione (codice di accesso e parola chiave per accedere ai computer e ai servizi web) attribuite alla S.V. e al personale sottoposto alla Sua direzione, controllo e coordinamento sono personali e devono essere custodite con cura e diligenza; non possono essere messe a disposizione né rivelate a terzi; non possono essere lasciate incustodite, né in libera visione. In caso di smarrimento e/o furto, bisogna darne immediata notizia al Delegato Interno (o, in caso di assenza di quest'ultimo, al Titolare) del trattamento dei dati;
8. nel caso in cui per l'esercizio delle attività sopra descritte sia inevitabile l'uso di supporti rimovibili (quali ad esempio chiavi USB, CD-ROM, ecc), su cui sono memorizzati dati personali, essi vanno custoditi con cura, mai messi a disposizione o lasciati al libero accesso di persone non autorizzate;
9. i supporti rimovibili contenenti dati sensibili e/o giudiziari, se non utilizzati, vanno distrutti o resi inutilizzabili;
10. l'accesso agli archivi contenenti dati sensibili o giudiziari è permesso solo alle persone autorizzate e soggetto a continuo controllo secondo le regole definite dalla scrivente;
11. durante i trattamenti i documenti contenenti dati personali vanno mantenuti in modo tale da non essere alla portata di vista di persone non autorizzate;
12. al termine del trattamento occorre sempre custodire i documenti contenenti dati personali all'interno di archivi/cassetti/armadi muniti di serratura;

13. i documenti della scuola contenenti dati personali non possono uscire dalla sede scolastica, né copiati, se non dietro espressa autorizzazione del Delegato Interno o dal Titolare del trattamento;
14. vigilare affinché, in caso di allontanamento anche temporaneo dal posto di lavoro, o comunque dal luogo dove vengono trattati i dati, l'incaricato abbia verificato che non vi sia possibilità da parte di terzi, anche se dipendenti non nominati Soggetti Autorizzati, di accedere a dati personali per i quali era in corso un qualunque tipo di trattamento;
15. le comunicazioni agli interessati (persone fisiche a cui afferiscono i dati personali) dovranno avvenire in forma riservata; se effettuate per scritto dovranno essere consegnate in contenitori chiusi;
16. all'atto della consegna di documenti contenenti dati personali l'incaricato dovrà assicurarsi dell'identità dell'interessato o di chi è stato delegato al ritiro del documento in forma scritta;
17. in caso di comunicazioni elettroniche ad alunni, colleghi, genitori, personale della scuola o altri soggetti coinvolti per finalità istituzionali, queste (comunicazioni) vanno poste in essere seguendo le indicazioni fornite dall'Istituzione scolastica e avendo presente la necessaria riservatezza delle comunicazioni stesse e dei dati coinvolti.

Nell'ambito delle istruzioni di cui sopra e nell'espletamento delle attività di Sua competenza, la S.V. è autorizzata a trattare direttamente i dati personali contenuti nelle banche dati elettroniche e negli archivi cartacei relativi a tutti i trattamenti effettuati da questo Istituto, fatti salvi i casi in cui la visione e il trattamento di alcuni dati è riservato in via esclusiva al Dirigente Scolastico.

REGISTRO DEI TRATTAMENTI

Rientra nelle Sue competenze supportare le competenti funzioni dell'Istituto e il DPO nella regolare tenuta del Registro dei Trattamenti. A questo fine, la S.V. dovrà comunicare al DPO ogni utile informazione relativamente ai trattamenti di dati personali svolti all'interno della Funzione da Lei presieduta, così come ogni modifica riguardante tali trattamenti e gli strumenti attraverso cui vengono svolti, oltre che i terzi eventualmente coinvolti.
Sarà Suo compito, inoltre, accertarsi dell'essenzialità e della pertinenza di tali dati ai fini del perseguimento delle finalità specifiche della funzione di Sua competenza. Qualora verificasse l'assenza di queste prerogative (essenzialità e pertinenza) dovrà provvedere, previo consulto con il DPO, a porre fine ai relativi trattamenti, procedendo alla cancellazione dei dati interessati, salvo che la legge ne imponga l'ulteriore conservazione per altre finalità amministrative, contabili e istituzionali.

GESTIONE DI ISTANZE DI INTERESSATI

La gestione delle istanze degli interessati è affidata al DPO che nello svolgimento di questa attività necessiterà della fattiva e competente collaborazione del Titolare e del Delegato Interno al Trattamento.
Nel caso in cui un Interessato faccia pervenire, nella funzione di Sua competenza, richieste riconducibili ai diritti a quest'ultimo garantiti dalla normativa vigente, Lei è tenuto ad informare senza ritardo il DPO e a fornire la Sua collaborazione per l'evasione della richiesta, attenendosi alle istruzioni operative che riceverà a tal riguardo.
Per quanto concerne dati o richieste che possono riguardare la funzione di Sua competenza, Lei dovrà fare in modo di assicurare che le operazioni di ricerca delle informazioni di cui il Titolare è in possesso siano rapide e complete, nel rispetto delle policy applicabili.
Roma, lì

Il Dirigente Scolastico
(Prof.ssa Patrizia Tozi)

Per accettazione

ALLEGATO 4: NOMINA A SOGGETTO AUTORIZZATO AL PERSONALE ATA.

INCARICO A SOGGETTO AUTORIZZATO AL TRATTAMENTO DEI DATI PERSONALI
a sensi dell'art. 29 del Regolamento (UE) 2016/679

L'Istituto Comprensivo Statale "Tullio De Mauro", con codice fiscale 97567160581, in qualità di Titolare del trattamento dei dati personali nella persona del Dirigente Scolastico Dott.ssa Patrizia Tozi:

DESIGNA

il/la Sig./a _____ c.f. _____, quale soggetto autorizzato al trattamento e incaricato del trattamento preposto allo svolgimento delle mansioni a Lei assegnate che comportano anche il trattamento di dati personali.

Quale persona autorizzata al trattamento dei dati personali sotto l'autorità diretta del Titolare, per le finalità collegate al corretto adempimento delle proprie mansioni di personale amministrativo, tecnico e ausiliario (di seguito personale ATA ai sensi del d.lgs. 16 aprile 1994, n. 297), potrà accedere ai dati personali delle persone fisiche che entreranno in rapporto con l'istituto scolastico a vario titolo.

Nello svolgimento della propria attività il soggetto incaricato del trattamento dovrà:

- attenersi scrupolosamente alle presenti e future istruzioni impartite dal Titolare o dal RPD;
- procedere al trattamento dei dati personali secondo gli ordini di servizio e nel rispetto dei principi generali di liceità, correttezza, trasparenza, esattezza e minimizzazione e delle prescrizioni contenute nel D.M. n. 305/2006;
- trattare i dati personali in modo lecito, corretto e trasparente nei confronti dell'interessato;
- raccogliere tali dati solo per finalità determinate, esplicite e legittime, e successivamente trattarli in modo compatibile con tali finalità;
- verificare che i dati siano adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
- verificare che i dati siano esatti e, se necessario, provvedere al loro aggiornamento;
- conservare i dati personali solo in base alle istruzioni ricevute e non per altre finalità;
- trattare i dati in modo integro e riservato garantendo, per quanto di propria competenza, un'adeguata sicurezza degli stessi in modo da ridurre il rischio di trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali;
- comunicare i dati personali dell'interessato solo all'interessato salvo che non vi sia una esplicita richiesta dell'interessato stesso oppure un obbligo legale oppure la comunicazione sia necessaria per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
- rispettare il divieto assoluto di divulgazione in qualunque forma o modalità, analogica o digitale, dei dati trattati nel corso del presente incarico, anche per il tempo successivo alla sua cessazione, senza limiti temporali.

In particolare, il soggetto autorizzato e incaricato del trattamento dovrà attenersi alle seguenti istruzioni:

1. non è mai consentito al soggetto autorizzato e incaricato del trattamento condividere la componente riservata delle proprie credenziali di autenticazione ai sistemi informativi con terzi. Le credenziali attribuite al soggetto autorizzato e incaricato non possono mai essere riprodotte su supporto cartaceo, né archiviate in altro modo in luoghi o supporti accessibili a terzi;
2. gli strumenti di lavoro eventualmente in possesso e uso esclusivo del soggetto incaricato (ad es. pc, notebook, ecc.) devono sempre essere protetti da sistemi di autenticazione, inattivati automaticamente a seguito del loro prolungato inutilizzo, e, per quanto possibile, non devono mai essere lasciati incustoditi se non temporaneamente per esigenze operative ed in ogni caso devono essere protetti, specie durante le sessioni di trattamento dei dati, da accessi non autorizzati attraverso sistemi di

autenticazione attivati automaticamente a seguito del loro prolungato inutilizzo (ad es. mediante screensaver);
3. potrà accedere alle banche dati degli alunni/famiglie nell'ambito dei trattamenti consentiti dalle mansioni di personale ATA da Lei svolte nell'istituto, sia con strumenti elettronici, sia in formato cartaceo;
4. non è consentito consultare caselle di posta elettronica personali mediante i computer e/o dispositivi dell'istituto, ed è fatto divieto di copia sugli stessi di altri dati e/o immagini strettamente personali;
5. nessun dato può essere utilizzato o trasmesso all'esterno in qualunque forma se non previa autorizzazione del Titolare del trattamento, ove tale utilizzo o trasmissione non siano previsti dalla funzione ricoperta o dall'attività svolta;
6. laddove impartite, seguire le indicazioni del Titolare circa le procedure di salvataggio dei dati personali;
7. ogni incaricato è tenuto ad osservare tutte le misure di protezione e sicurezza atte ad evitare rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta, già in atto o che, in futuro, venissero indicate dal Titolare del trattamento;
8. gli atti e i documenti contenenti dati personali devono essere utilizzati e custoditi con diligenza e non devono essere mai essere lasciati incustoditi, se non temporaneamente per esigenze documentabili, e al termine del loro utilizzo devono essere riposti in luoghi accessibili solo al personale autorizzato e protetti da misure di sicurezza fisiche;
9. partecipare agli interventi formativi organizzati dall'istituzione scolastica sui profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle attività connesse alle sue mansioni.
10. se presenti, l'incaricato dovrà attenersi obbligatoriamente a linee guida e istruzioni operative dell'istituto scolastico.

Il Titolare del trattamento si riserva il diritto di aggiornare le istruzioni impartite al soggetto autorizzato e incaricato del trattamento e di eseguire controlli per verificare che tali attività si svolgano secondo le istruzioni ricevute e le disposizioni di legge.

La presente nomina è a tempo indeterminato e s'intende automaticamente revocata alla data di cessazione del rapporto di lavoro in essere con questa istituzione scolastica.

Sottoscrivendo la presente comunicazione attesta la presa visione in accettazione di quanto riportato, nonché di aver partecipato ad una sessione formativa in tema di protezione dei dati personali e diritto alla privacy ai sensi del Regolamento (UE) n. 2016/679 e successive norme nazionali di adeguamento.

Il Dirigente Scolastico
(Prof.ssa Patrizia Tozi)

Roma, lì

Letto e sottoscritto per accettazione

Il soggetto autorizzato:

_____

ALLEGATO 5: NOMINA A SOGGETTO AUTORIZZATO AL PERSONALE DOCENTE

INCARICO A SOGGETTO AUTORIZZATO Al SENSI DELL'ART. 29 DEL REGOLAMENTO UE 2016/679 E SUCCESSIVE NORME NAZIONALI DI ADEGUAMENTO

L'Istituto Comprensivo Statale "Tullio De Mauro", con codice fiscale 97567160581, in qualità di Titolare del trattamento dei dati personali nella persona del Dirigente Scolastico Dott.ssa Patrizia Tozi:

DESIGNA

il/la Prof./ssa _____ c.f. _____, quale soggetto autorizzato al trattamento e incaricato del trattamento preposto allo svolgimento delle mansioni a Lei assegnate che comportano anche il trattamento di dati personali.

Quale persona autorizzata al trattamento dei dati personali sotto l'autorità diretta del Titolare, per le finalità collegate al corretto adempimento delle proprie mansioni di personale docente, potrà accedere ai dati personali delle persone fisiche che entreranno in rapporto con l'istituto scolastico a vario titolo.

Nello svolgimento della propria attività il soggetto incaricato del trattamento dovrà:

- attenersi scrupolosamente alle presenti e future istruzioni impartite dal Titolare o dal RPD;
- procedere al trattamento dei dati personali secondo gli ordini di servizio e nel rispetto dei principi generali di liceità, correttezza, trasparenza, esattezza e minimizzazione e delle prescrizioni contenute nel D.M. n. 305/2006, e in particolar modo delle schede, ad esso allegate, n.4 (attività propedeutiche all'inizio dell'anno scolastico) e n.5 (attività educativa, didattica e formativa, di valutazione);
- trattare i dati personali in modo lecito, corretto e trasparente nei confronti dell'interessato;
- raccogliere tali dati solo per finalità determinate, esplicite e legittime, e successivamente trattarli in modo compatibile con tali finalità;
- verificare che i dati siano adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
- verificare che i dati siano esatti e, se necessario, provvedere al loro aggiornamento;
- conservare i dati personali solo in base alle istruzioni ricevute e non per altre finalità;
- trattare i dati in modo integro e riservato garantendo, per quanto di propria competenza, un'adeguata sicurezza degli stessi in modo da ridurre il rischio di trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali;
- comunicare i dati personali dell'interessato solo all'interessato salvo che non vi sia una esplicita richiesta dell'interessato stesso oppure un obbligo legale oppure la comunicazione sia necessaria per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
- rispettare il divieto assoluto di divulgazione in qualunque forma o modalità, analogica o digitale, dei dati trattati nel corso del presente incarico, anche per il tempo successivo alla sua cessazione, senza limiti temporali.
- In particolare, il soggetto autorizzato e incaricato del trattamento dovrà attenersi alle seguenti istruzioni:
- non è mai consentito al soggetto autorizzato e incaricato del trattamento condividere la componente riservata delle proprie credenziali di autenticazione ai sistemi informativi con terzi. Le credenziali attribuite al soggetto autorizzato e incaricato non possono mai essere riprodotte su supporto cartaceo, né archiviate in altro modo in luoghi o supporti accessibili a terzi;
- gli strumenti di lavoro eventualmente in possesso e uso esclusivo del soggetto incaricato (ad es. pc, notebook, ecc.) devono sempre essere protetti da sistemi di autenticazione, inattivati automaticamente a seguito del loro prolungato inutilizzo, e, per quanto possibile, non devono mai essere lasciati incustoditi se non temporaneamente per esigenze operative ed in ogni caso devono essere protetti, specie durante le sessioni di trattamento dei dati, da accessi non autorizzati attraverso sistemi di autenticazione attivati automaticamente a seguito del loro prolungato inutilizzo (ad es. mediante screensaver);

- potrà accedere alle banche dati degli alunni/famiglie nell'ambito dei trattamenti consentiti dalle mansioni di personale docente da Lei svolte nell'istituto, sia con strumenti elettronici, sia in formato cartaceo;
- non è consentito consultare caselle di posta elettronica personali mediante i computer e/o dispositivi dell'istituto, ed è fatto divieto di copia sugli stessi di altri dati e/o immagini strettamente personali;
- nessun dato può essere utilizzato o trasmesso all'esterno in qualunque forma se non previa autorizzazione del Titolare del trattamento, ove tale utilizzo o trasmissione non siano previsti dalla funzione ricoperta o dall'attività svolta;
- laddove impartite, seguire le indicazioni del Titolare circa le procedure di salvataggio dei dati personali;
- ogni incaricato è tenuto ad osservare tutte le misure di protezione e sicurezza atte ad evitare rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta, già in atto o che, in futuro, venissero indicate dal Titolare del trattamento;
- gli atti e i documenti contenenti dati personali devono essere utilizzati e custoditi con diligenza e non devono essere mai essere lasciati incustoditi, se non temporaneamente per esigenze documentabili, e al termine del loro utilizzo devono essere riposti in luoghi accessibili solo al personale autorizzato e protetti da misure di sicurezza fisiche;
- partecipare agli interventi formativi organizzati dall'istituzione scolastica sui profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle attività connesse alle sue mansioni.
- se presenti, l'incaricato dovrà attenersi obbligatoriamente a linee guida e istruzioni operative dell'istituto scolastico.
- Il Titolare del trattamento si riserva il diritto di aggiornare le istruzioni impartite al soggetto autorizzato e incaricato del trattamento e di eseguire controlli per verificare che tali attività si svolgano secondo le istruzioni ricevute e le disposizioni di legge.

La presente nomina è a tempo indeterminato e s'intende automaticamente revocata alla data di cessazione del rapporto di lavoro in essere con questa istituzione scolastica.

Sottoscrivendo la presente comunicazione attesta la presa visione in accettazione di quanto riportato, nonché di aver partecipato ad una sessione formativa in tema di protezione dei dati personali e diritto alla privacy ai sensi del Regolamento Europeo n. 679/2016 e successive norme nazionali di adeguamento.

Roma, lì

Il Dirigente Scolastico
(Prof.ssa Patrizia Tozi)

Roma, lì

Letto e sottoscritto per accettazione

Il soggetto autorizzato:

Prof./ssa

_____

Accordo di NOMINA A RESPONSABILE ESTERNO DEL TRATTAMENTO DEI DATI PERSONALI

Spett.le
XXXXXXXXXXXXXXXXXXX
Via XXXXXXXXXXXXXXXX XXX
CAP Comune (PV)
P.IVA: XXXXXXXXXXX
CF: XXXXXXXXXXXXXXX

Oggetto: Accordo sul trattamento dei Dati Personali connesso all'erogazione dei servizi in favore del L'istituto Comprensivo Statale "Tullio De Mauro", Titolare del trattamento dei dati personali, ai sensi della vigente normativa sulla protezione dei dati personali art. 28 del Regolamento 2016/679/UE (nel seguito anche "GDPR")

Premesso che:

- è in corso un rapporto contrattuale tra le nostre società (per brevità detto anche il "Contratto"), finalizzato all'erogazione di servizi per l'Istituto Comprensivo Statale "Tullio De Mauro", con sede legale in Viale Fernando Santi, 65 - 00155 ROMA, nella persona del Dirigente Scolastico Prof.ssa Patrizia Tozi, (di seguito il "titolare), relativi al trattamento dei dati personali denominato xxxxx (per brevità detti anche "Servizi") da parte di XXXXXXXXXXXXXXXXXXXXX detta anche "Fornitore" e, congiuntamente con Titolare, le "Parti");
    - ai sensi della vigente normativa europea ed italiana in materia di protezione dei dati personali (la "Normativa Privacy"), l'esecuzione dei Servizi comporta, da parte di XXXXXXXXXXXXXXXX, il trattamento di dati personali per conto dell'Istituto Comprensivo "Tullio De Mauro":
    - a mezzo della presente le Parti intendono disciplinare il trattamento dei dati personali effettuato dal Fornitore quale Responsabile del trattamento nell'esecuzione dei Servizi di cui al Contratto, ai sensi della normativa sulla protezione dei dati personali.

Tutto ciò premesso, tra le Parti si conviene e stipula quanto segue:

- Le Parti, con riferimento alle attività di trattamento dei dati personali connesse alla fornitura dei Servizi di cui al Contratto, concordano che tali attività sono svolte dal Fornitore per conto del Titolare del trattamento e che il Fornitore agisce in qualità di Responsabile di tale trattamento, ex art. 28 del GDPR.
- Le Parti si danno reciprocamente atto che la fornitura dei Servizi comporta il trattamento dei dati personali appartenenti alle categorie meglio descritte nelle schede di trattamento allegate in calce al presente contratto, di cui fanno parte integrante, ove sono pure riportate le finalità, le basi di liceità, la durata e tutti gli altri elementi previsti dal registro trattamenti, così come contrattualmente convenuto e meglio indicato dal Contratto/Accordo, del quale il presente Atto costituisce appendice integrante, nonché come descritto nel seguito.
- Il Fornitore, in qualità di Responsabile, conferma di presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento risponda ai requisiti prescritti al fine di garantire la tutela dei dati personali e i diritti degli interessati.
- il Fornitore si impegna a rispettare gli obblighi che le disposizioni del GDPR e del D. lgs. 196/03, come modificato dal D. lgs. 101/18, pongono direttamente a carico del Responsabile del trattamento:
    - effettuare le operazioni di trattamento dei suddetti dati personali nel pieno rispetto dei principi e delle disposizioni della vigente normativa sulla protezione dei dati personali ed esclusivamente ai fini dell'esecuzione dei Servizi, secondo le modalità, procedure e modulistiche via via indicate dal Titolare;
    - trattare i dati personali soltanto sulla base delle documentate istruzioni fornite del Titolare, anche in caso di eventuale trasferimento di dati personali verso soggetti stabiliti in Paesi al di fuori della UE, che potrà essere effettuato solo previa autorizzazione del Titolare medesimo e sulla base delle relative istruzioni, adottando le adeguate garanzie secondo la vigente normativa europea e nazionale di riferimento, garanzie di cui andrà mantenuta adeguata documentazione da fornire, ove richiesto, dal Titolare;

- adottare tutte le misure richieste per la sicurezza del trattamento, ai sensi dell'art. 32 del GDPR nonché dei provvedimenti prescrittivi del Garante in tema di sicurezza dei dati ed amministratori di sistema fino alla loro eventuale modifica, sostituzione ed abrogazione, successivamente al 25 maggio 2018;
- assistere il Titolare nel garantire il rispetto, per quanto di relativa competenza, degli obblighi in tema di sicurezza, notifica all'Autorità per la protezione dei dati personali (nel seguito "Garante") di eventuali violazioni di dati personali e, se del caso, loro comunicazione agli interessati, nonché di valutazione d'impatto sulla protezione dati ed eventuale consultazione preventiva, ai sensi degli articoli da 32 a 36 del GDPR, tenendo conto della natura del trattamento e delle informazioni a disposizione dello stesso Responsabile, nonché delle documentate istruzioni via via impartite dal Titolare in relazione all'adempimento dei suddetti obblighi;
- individuare le persone autorizzate al trattamento dei dati personali (gli Incaricati), che operano sotto l'autorità del medesimo Fornitore, nonché adottare le misure volte a garantire l'assunzione da parte di tali persone di idonei obblighi di riservatezza in ordine ai dati personali trattati, fornire loro adeguate e documentate istruzioni circa il rispetto, in particolare, delle misure per la sicurezza dei dati e vigilare sulla osservanza, da parte delle persone autorizzate, delle istruzioni impartite per il trattamento dei dati personali e delle vigenti disposizioni normative in materia di protezione dei dati personali;
- assicurare, ai fini della corretta applicazione della vigente normativa sulla privacy, il costante monitoraggio degli adempimenti e delle attività effettuati da chi opera sotto la propria autorità (se applicabili: fornire l'informativa, raccogliere il consenso, l'elaborazione ed archiviazione, la comunicazione e la diffusione, etc.) in relazione alle operazioni di trattamento di competenza;
- informare periodicamente il Titolare, su richiesta di quest'ultimo, in ordine all'attività svolta, sia sotto il profilo del trattamento, sia sotto il profilo della sicurezza dei dati;
- conservare i dati in una forma che consenta l'identificazione degli interessati per un periodo di tempo non superiore a quello necessario agli scopi per i quali sono stati raccolti e successivamente trattati;
- inviare al Titolare previa apposita richiesta scritta, al momento della cessazione delle operazioni di trattamento o anche antecedentemente in caso di specifica richiesta del Titolare, la documentazione comprovante l'avvenuta esecuzione degli adempimenti privacy;
- informare prontamente il Titolare di ogni questione rilevante ai fini della presente nomina, quali a titolo indicativo: istanze di interessati; richieste del Garante; violazioni o messa in pericolo della riservatezza, della completezza o dell'integrità dei dati personali.
- fornire per quanto di competenza la massima collaborazione al Titolare in caso di istanze avanzate da parte degli interessati, ex artt. dal 15 al 22 del GDPR, le cui informazioni sono trattate in esecuzione dei Servizi o in caso di accertamenti o ispezioni effettuate da parte del Garante, nonché in caso di qualsiasi controversia avente ad oggetto la normativa a tutela dei dati personali;
- garantire per quanto di competenza l'esecuzione di ogni altra operazione richiesta o necessaria per ottemperare agli obblighi derivanti dalle disposizioni di legge e/o da regolamenti vigenti in materia di protezione dei dati personali;
- mettere a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente Atto ed alla vigente Normativa Privacy, nonché consentire e contribuire alle attività di revisione, comprese le ispezioni che il Titolare (con preavviso minimo di 5 giorni), direttamente o avvalendosi di terzi, potrà effettuare per verificare la puntuale osservanza di quanto previsto dalla vigente normativa in materia di protezione dei dati personali nonché delle proprie indicazioni.

- Con riferimento al trattamento dei dati personali connesso alla fornitura dei Servizi di cui al Contratto, il Titolare autorizza il Fornitore ad avvalersi degli ulteriori responsabili informando tempestivamente il Titolare, che potrà manifestare la sua opposizione entro 15 giorni dal ricevimento di tale comunicazione. Il Responsabile si impegna a che tali ulteriori responsabili posseggano competenze, conoscenze ed esperienze sufficienti per mettere in atto misure tecniche e organizzative idonee a garantire il rispetto delle disposizioni del GDPR. Il Responsabile si impegna, nell'ambito dei contratti od accordi stipulati con gli ulteriori responsabili, a:
    - vincolare contrattualmente gli ulteriori responsabili al rispetto degli stessi obblighi in materia di protezione dei dati personali assunti dal Responsabile nei confronti del Titolare, ove applicabili e pertinenti rispetto alle attività a questi ultimi affidate;
    - custodire copia dei predetti contratti, accordi o documenti disciplinanti gli obblighi in materia di protezione dei dati personali, sottoscritti per presa visione ed accettazione da parte degli ulteriori responsabili e fornirne copia al Titolare, su sua richiesta;
    - assumere nei confronti del Titolare ogni responsabilità in ordine al rispetto dei predetti obblighi da parte degli ulteriori responsabili;

- L'esecuzione delle attività di cui al presente accordo non originano alcun diritto del Responsabile a percepire compensi ulteriori rispetto a quanto previsto per i Servizi.
- Il Responsabile si impegna a tenere indenne il Titolare da ogni responsabilità, costo, spesa o altro onere, discendenti da pretese, azioni o procedimenti di terzi a causa della violazione, da parte del Responsabile (o di suoi dipendenti o collaboratori ovvero degli ulteriori responsabili), degli obblighi a suo carico in base alla presente e/o della violazione delle prescrizioni di cui alla vigente normativa in materia di protezione dei dati personali.
- Alla cessazione per qualsiasi causa dei Servizi, il Responsabile sarà tenuto, a discrezione del Titolare: a restituire al Titolare i dati personali oggetto del trattamento oppure a provvedere alla loro integrale distruzione, salvi solo i casi in cui la conservazione dei dati sia richiesta da norme di legge ad altri fini (contabili, fiscali, ecc.). In entrambi i casi il Responsabile provvederà a rilasciare al Titolare apposita dichiarazione per iscritto contenente l'attestazione che presso il Responsabile non esiste alcuna copia dei dati personali e delle informazioni di titolarità del Titolare, fatti salvi i casi in cui la conservazione dei dati sia richiesta da norme di legge ad altri fini (contabili, fiscali, ecc.). Il Titolare si riserva il diritto di effettuare controlli e verifiche volte ad accertare la veridicità della dichiarazione.
- La presente nomina va intesa come se fosse stata effettuata all'inizio del rapporto contrattuale tra le nostre Società ed avrà durata fino alla cessazione, per qualsivoglia motivo, dello stesso.

Luogo e Data

Il Dirigente Scolastico
(Prof.ssa Patrizia Tozi)

Presa visione e accettazione

_____

_____

ALLEGATO 7: INFORMAZIONI SUL TRATTAMENTO FORNITE AI DIPENDENTI

INFORMAZIONI SUL TRATTAMENTO DEI DATI PERSONALI – RAPPORTO DI LAVORO

Ai sensi e per gli effetti dell'art.13 del Regolamento (UE) 2016/679

Ai sensi del Regolamento (UE) General Data Protection Regulation "GDPR" n. 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 (di seguito il "Regolamento" o "GDPR"), considerando le disposizioni del d.lgs. 196/2003 c.d. Codice privacy, così come novellato dal d.lgs. 101/2018, la informiamo che i dati personali forniti all'Istituto scolastico saranno trattati secondo i principi di liceità, correttezza e trasparenza al fine di garantire i diritti, le libertà fondamentali, nonché la dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale. La presente informativa descrive le modalità di trattamento.

ESTREMI IDENTIFICATIVI DEL TITOLARE DEL TRATTAMENTO DATI PERSONALI

Il Titolare del Trattamento, (di seguito "Titolare") è l'Istituto Comprensivo Statale "Tullio De Mauro", con sede legale in Viale Fernando Santi, 65 - 00155 ROMA, nella persona del Dirigente Scolastico Prof.ssa Patrizia Tozi.
Dati di contatto: Tel. +39 06/ 95955067, E-mail: rmic8b5008@istruzione.it - PEC: rmic8b5008@pec.istruzione.it

RESPONSABILE PER LA PROTEZIONE DEI DATI PERSONALI

Ai sensi dell'art. 37 del Regolamento, il Titolare ha designato il Responsabile della Protezione dei Dati personali (RPD) o anche Data Protection Officer (DPO) nella persona di Massimo Corinti.
Dati di contatto: Mob. +39 335 7687380 - E-mail: dpo@corinti.eu - PEC: dpo@pec.corinti.eu

FINALITÀ E BASI GIURIDICHE DEL TRATTAMENTO

I Suoi dati personali sono trattati per l'adempimento degli obblighi legali tutti e contrattuali, anche collettivi, connessi al rapporto di lavoro, di seguito meglio specificati:

1. dati idonei a rilevare lo stato di salute contenuti in certificati per malattia, infortuni, maternità, appartenenza a categorie protette, adempimenti sanitari in materia di sicurezza sul lavoro;
2. dati idonei a rilevare opinioni politiche o adesioni a partiti politici e/o sindacati con particolare riferimento alla fruizione di permessi o aspettative previste da disposizioni di legge, gestione delle ritenute e versamenti di quote associative a partiti politici e sindacati;
3. dati idonei a rilevare le convinzioni religiose o l'adesione ad organizzazioni religiose e la fruizione di permessi in tal senso o la destinazione di somme a tali organizzazioni.
4. elaborazione, liquidazione e corresponsione delle spettanze e relativa contabilizzazione;
5. adempimenti previsti da disposizione di legge e regolamentari in materia previdenziale, fiscale, assicurativa e di sicurezza sul lavoro;
6. tutela dei diritti nelle sedi giudiziarie;

La base giuridica per le suddette finalità:

- è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
- necessario per il perseguimento del legittimo interesse del titolare del trattamento per adempimenti di obblighi fiscali e contabili a cui è soggetto il titolare del trattamento.
- Art. 9 par. 2 lett. b) Necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro, della sicurezza e protezione.

Considerato inoltre, le indicazioni per la gestione di casi e focolai di SARS-CoV-2 nelle scuole e nei servizi educativi dell'infanzia stabilite nel "Rapporto IIS COVID-19 n.58/2020 del 20/08/2020", nel caso in cui si presentino sintomatologie compatibili con COVID-19 in ambito scolastico, l'Istituto, per tramite del referente scolastico COVID-19, fornirà al Dipartimento di Prevenzione (DdP) l'elenco dei soggetti del caso confermato, che sono stati a contatto nelle 48 ore precedenti l'insorgenza dei sintomi, al fine di espletare le attività di contact tracing (ricerca e gestione dei contatti).

CATEGORIE DEI DATI TRATTATI

Nei limiti delle finalità e delle modalità descritte nelle presenti Informazioni, potranno essere trattati dati che possono essere considerate come dati "personali comuni", nei quali rientrano le generalità, l'anagrafica completa, il codice fiscale. Come dati particolari "sensibili", ai sensi dell'art. 9 par. 2 lett. b), il documento di identità, i numeri di utenza telefonica, sia essa fissa o mobile, l'indirizzo e-mail, le coordinate bancarie, l'idoneità al lavoro, lo stato di salute, Informazioni di carattere giudiziario, ai sensi dell'art. 4 comma 1, lett. e) del d.lgs 196/2003.

Il Titolare potrà inoltre trattare i dati per immagini, foto e riprese audio-video all'interno dell'attività educativa e didattica, per scopi formativi e informativi, da affiggere all'interno dell'Istituto scolastico o da pubblicare sul sito web istituzionale, il trattamento avrà natura temporanea ovvero, per il tempo necessario per le finalità a cui sono destinati. Inoltre, il Titolare ogni qualvolta si dovesse presentare la necessità di effettuare foto o riprese audio-video afferenti a specifici progetti, presenterà una specifica informativa. Per tutti i trattamenti di dati per immagine sarà richiesto un apposito consenso facoltativo e liberamente espresso da parte delle famiglie.

MODALITA' DI TRATTAMENTO E TRATTAMENTI AUTOMATIZZATI

I dati personali forniti all'Istituto, saranno trattati nel nell'osservanza e nel rispetto della normativa GDPR e degli obblighi di riservatezza e liceità cui è ispirata l'attività del Titolare. I dati verranno trattati sia su supporti cartacei sia attraverso strumenti informatici per lo svolgimento delle attività educative. In merito alla piattaforma G Suite for Education, ed in particolare Google Meet utilizzato per videoconferenza, è stato verificato il rispetto delle normative in materia di protezione dei dati personali da parte del fornitore. La Piattaforma Google Cloud Platform utilizza la crittografia come impostazione predefinita ed è applicata durante il transito dei dati tra il cliente e Google, nel caso di Meet, funziona interamente nel browser limitando l'esposizione ad eventuali attacchi informatici.
Non esistono processi decisionali automatizzati e non viene attuata una profilazione dei dati.

DIFFUSIONE, COMUNICAZIONE E SOGGETTI CHE ACCEDONO AI DATI

La informiamo che i Soggetti, ai quali i dati possono essere comunicati sono esclusivamente quelli previsti dalla legge e/o da regolamenti – Regolamento del MPI, Enti pubblici (INPS, Direzione provinciale del lavoro, Uffici fiscali... etc.), fondi o casse anche private di previdenza e assistenza, studi medici in adempimento degli obblighi in materia di igiene e sicurezza del lavoro, organizzazioni sindacali cui lei abbia conferito specifico mandato, fondi integrativi.
Da ultimo, la comunicazione dei dati personali potrà essere effettuata verso enti e/o autorità pubbliche in base agli obblighi previsti dalla legge e/o da regolamenti, in particolare per la gestione di eventuali casi e focolai di SARS-CoV-2 nelle scuole, i dati verranno comunicati al Dipartimento di Prevenzione (DdP);
L'istituto non trasferisce dati personali in paesi terzi extra UE o ad organizzazioni internazionali, qualora ciò si rivelasse necessario ai fini istituzionali, per lo svolgimento delle attività educative ed istituzionali, per la fruizione della Didattica Digitale Integrata, l'Istituto verificherà che sussistano tutti i presupposti giuridici per assicurare un adeguato livello di protezione.

DURATA DEL TRATTAMENTO E CONSERVAZIONE DEI DATI PERSONALI

Non è prevista la distruzione o cancellazione dai dati personali trattati nell'ambito del rapporto di lavoro con l'istituto, salvo esplicita richiesta di cancellazione da parte dell'interessato; in ogni caso taluni dati potranno essere conservati eventualmente in base alle scadenze previste dalle vigenti norme di legge.

DIRITTI DELL'INTERESSATO

Contattando il Titolare, per tramite del Responsabile della Protezione dei Dati, l'interessato può esercitare i diritti previsti di cui agli artt. da 15 a 22 e per quanto applicabili in considerazione dell'art. 23 del Regolamento. Laddove richiesto, l'interessato ha il diritto di accesso ai propri dati personali, alla rettifica dei dati inesatti, alla cancellazione, alla limitazione o alla possibilità di opporsi al trattamento, di richiedere la portabilità dei dati, di revocare il consenso. La risposta alle richieste sarà fornita entro un mese, se la richiesta è troppo complessa o in presenza di numerose richieste tale periodo può prorogarsi di altri due mesi.
Inoltre, l'interessato ha sempre il diritto di proporre reclamo al Garante ai riferimenti presenti nel sito web: www.garanteprivacy.it, o di adire le opportune sedi giudiziarie.

Aggiornamento ottobre 2022

IL DIRIGENTE SCOLASTICO

(Prof.ssa Patrizia Tozi)

CONSENSO AL TRATTAMENTO DEI DATI PERSONALI

Il/La sottoscritto/a _____, preso atto delle presenti informazioni rese dal Titolare, ai sensi degli art. 13 e 14 del GDPR, esprime il suo consenso per la seguente finalità:

Per il trattamento dei dati per immagini all'interno di attività educative e didattiche per scopi formativi e informativi.	☐ Presto il consenso ☐ Nego il consenso
Dichiaro di aver preso visione dell'informativa elativa al trattamento denominato: "Trattamenti indispensabili per il rapporto di lavoro"	☐ Presto il consenso

Roma, lì_____ Nome, Cognome, Firma dell'interessato

_____

ALLEGATO 8: INFORMAZIONI SUL TRATTAMENTO FORNITE AGLI ALUNNI.

INFORMAZIONI SUL TRATTAMENTO DEI DATI PERSONALI DEGLI STUDENTI E DELLE FAMIGLIE

Ai sensi e per gli effetti dell'art. 13 del Regolamento (UE) 2016/679

Ai sensi del Regolamento (UE) General Data Protection Regulation "GDPR" n. 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 (di seguito il "Regolamento" o "GDPR"), considerando le disposizioni del d.lgs. 196/2003 c.d. Codice privacy, così come novellato dal d.lgs. 101/2018, la informiamo che i dati personali forniti all'Istituto scolastico saranno trattati secondo i principi di liceità, correttezza e trasparenza al fine di garantire i diritti, le libertà fondamentali, nonché la dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale. La presente informativa descrive le modalità di trattamento.

ESTREMI IDENTIFICATIVI DEL TITOLARE DEL TRATTAMENTO DATI PERSONALI

Il Titolare del Trattamento, (di seguito "Titolare") è l'Istituto Comprensivo Statale "Tullio De Mauro", con sede legale in Viale Fernando Santi, 65 - 00155 ROMA, nella persona del Dirigente Scolastico Prof.ssa Patrizia Tozi.
Dati di contatto: Tel. +39 06/ 95955067, E-mail: rmic8b5008@istruzione.it - PEC: rmic8b5008@pec.istruzione.it

RESPONSABILE PER LA PROTEZIONE DEI DATI PERSONALI

Ai sensi dell'art. 37 del Regolamento, il Titolare ha designato il Responsabile della Protezione dei Dati personali (RPD) o anche Data Protection Officer (DPO) nella persona di Massimo Corinti.
Dati di contatto: Mob. +39 335 7687380 - E-mail: dpo@corinti.eu - PEC: dpo@pec.corinti.eu

FINALITÀ E BASI GIURIDICHE DEL TRATTAMENTO

Ai sensi dell'art. 6 del Regolamento, in particolare al paragrafo 1, lettera e), considerando l'art. 2-ter del d.lgs. 101/2018, i dati personali di studenti e famiglie, sono trattati per l'assolvimento degli obblighi istituzionali dell'Istituto scolastico, in particolare, per la partecipazione alle attività educative, formative e di istruzione stabilite dal Piano dell'Offerta Formativa altresì per finalità strettamente connesse e strumentali alla gestione dei rapporti con gli alunni, per finalità connesse agli obblighi previsti da leggi e da regolamenti in materia di istruzione ed assistenza scolastica, per la tutela della salute degli studenti dell'Istituto nel contenimento e contrasto alla diffusione del SARS-CoV-2 e della malattia da coronavirus COVID-19, per l'attività didattica-formativa e valutazione e per le attività propedeutiche all'avvio dell'anno scolastico.
La base giuridica per le suddette finalità è l'esecuzione di un compito d'interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare. Per tali finalità non è richiesto il consenso dell'interessato.

CATEGORIE DEI DATI TRATTATI

Considerato i principi applicabili al trattamento dei dati personali previsti dall'art. 5 del Regolamento (UE), le categorie di dati personali di studenti e famiglie che potranno essere trattati dall'Istituto scolastico sono:

- Dati personali "comuni" nei quali rientrano, a titolo esemplificativo, le generalità, l'anagrafica completa, inclusi eventuali numeri di identificazione personale, i recapiti (ad es. numero di cellulare, indirizzo e-mail);
- Dati personali "particolari" che le istituzioni scolastiche sono autorizzate a trattare ai sensi dell'art. 9 paragrafo 2, lettera g) del Regolamento e considerando gli artt. 2-sexies comma 2 lettera bb) del d.lgs. 101/2018, indicando anche le operazioni ordinarie che i Titolari devono necessariamente svolgere per perseguire le finalità di rilevante interesse pubblico.

- Dati "giudiziari" ai sensi dell'art. 2-octies del d.lgs. 101/2018.

Nell'ambito del servizio "Pago in Rete", è prevista l'acquisizione ed associazione dei dati anagrafici del soggetto pagatore (alunno/a) e del soggetto versante (genitore o chi esercita la responsabilità genitoriale), nello specifico, i rispettivi codici fiscali, al fine di generare gli avvisi telematici intestati all'interno del Servizio "Pago In Rete" e, dunque, consentire i pagamenti richiesti e la fruizione del Servizio da parte dell'Istituzione scolastica.

Considerato le indicazioni per la gestione di casi e focolai di SARS-CoV-2 nelle scuole e nei servizi educativi dell'infanzia stabilite nel "Rapporto IIS COVID-19 n.58/2020 del 20/08/2020" s.m.i., nel caso in cui un alunno presenti un aumento della temperatura corporea al di sopra di 37,5 °C o un sintomo compatibile con COVID-19 in ambito scolastico, l'Istituto, per tramite del referente scolastico COVID-19, fornirà al Dipartimento di Prevenzione (DdP) l'elenco dei compagni di classe del caso confermato che sono stati a contatto nelle 48 ore precedenti l'insorgenza dei sintomi al fine di espletare le attività di contact tracing (ricerca e gestione dei contatti).

La informiamo inoltre che i dati personali di studenti e famiglie oggetto di trattamento, potranno essere:

a) nelle attività propedeutiche all'avvio dell'anno scolastico:

- dati relativi alle origini razziali ed etniche, per favorire l'integrazione degli alunni con cittadinanza non italiana;
- dati relativi alle convinzioni religiose, per garantire la libertà di credo religioso e per la fruizione dell'insegnamento della religione cattolica o delle attività alternative a tale insegnamento;
- dati relativi allo stato di salute e alla situazione vaccinale;
- per la gestione del percorso integrato per la somministrazione dei farmaci in ambito scolastico con riferimento al protocollo di intesa MIUR - Ufficio scolastico regionale per il Lazio e Regione Lazio per assicurare l'erogazione del sostegno e del servizio di assistenza specialistica e/o sensoriale.
- dati relativi alle vicende giudiziarie, per assicurare il diritto allo studio anche a soggetti sottoposti a regime di detenzione (i dati giudiziari emergono anche nel caso in cui l'autorità giudiziaria abbia predisposto un programma di protezione nei confronti degli alunni che abbiano commesso reati).

b) nell'espletamento dell'attività educativa, didattica, formativa e di valutazione:

- dati relativi alle origini razziali ed etniche per favorire l'integrazione degli alunni con cittadinanza non italiana;
- dati relativi alle convinzioni religiose per garantire la libertà di credo religioso;
- dati relativi allo stato di salute e alla situazione vaccinale, per assicurare l'erogazione del servizio di refezione scolastica, del sostegno agli alunni con disabilità o disturbi specifici dell'apprendimento (art.3 comma 1 e 3 della L. 104/92 e L. 170/2010), dell'insegnamento domiciliare ed ospedaliero nei confronti degli alunni affetti da gravi patologie, per la partecipazione alle attività educative e didattiche programmate, a quelle motorie e sportive, alle visite guidate e ai viaggi di istruzione;
- dati giudiziari, per assicurare il diritto allo studio anche a soggetti sottoposti a regime di detenzione;
- dati relativi all'esame dei provvedimenti atti a dimostrare l'esercizio della responsabilità genitoriale;

c) nella gestione del contenzioso tra la scuola e le famiglie degli alunni:

- dati sensibili e giudiziari concernenti tutte le attività connesse alla difesa in giudizio dell'Istituto scolastico.

d) nella gestione amministrativa specifica per studenti con disabilità:

gli studenti con disabilità necessitano di procedure amministrative atte a garantire tutte le tutele necessarie al soggetto interessato. Tali procedure coinvolgono una serie di trattamenti dei dati ai fini all'assegnazione degli insegnanti di sostegno, al mantenimento del fascicolo disabile cartaceo, alla creazione e al mantenimento della "partizione alunni disabili" della Anagrafe Nazionale degli Studenti (secondo quanto disposto dal Decreto MIUR 162 del 28 Luglio 2016 e successive circolari). A tal riguardo, si informa che su istanza dei genitori presentata al fine di ottenere l'assegnazione dell'insegnante di sostegno, i dati di salute di alunni affetti da gravi patologie o disabilità sono trasmessi per mail in forma cifrata agli uffici competenti e per via telematica ad una partizione specifica della banca dati denominata "Anagrafe Nazionale degli Studenti". Da questa partizione accederà, in sola lettura e in forma anonima, il personale autorizzato dagli Enti preposti all'erogazione del servizio. I dati trattati sono dati afferenti al Piano Educativo Individuale.

Il Titolare potrà inoltre trattare i dati per immagini, foto e riprese audio-video all'interno dell'attività educativa e didattica, per scopi formativi e informativi, da affiggere all'interno dell'Istituto scolastico o da pubblicare sul sito web istituzionale, il trattamento avrà natura temporanea ovvero, per il tempo necessario per le finalità a cui sono destinati. Inoltre, il Titolare ogni qualvolta si dovesse presentare la necessità di effettuare foto o riprese audio-video afferenti a specifici progetti, invierà una specifica informativa. Per tutti i trattamenti di dati per immagine sarà richiesto un apposito consenso facoltativo e liberamente espresso da parte delle famiglie.

MODALITA' DI TRATTAMENTO E TRATTAMENTI AUTOMATIZZATI

I dati personali forniti all'Istituto, saranno trattati nel nell'osservanza e nel rispetto della normativa GDPR e degli obblighi di riservatezza e liceità cui è ispirata l'attività del Titolare. I dati verranno trattati sia su supporti cartacei sia attraverso strumenti informatici per lo svolgimento delle attività educative. È necessario porre alla sua attenzione il fatto che l'istituto alimenta e aggiorna continuamente l'Anagrafe Nazionale degli Studenti, ospitata dalla piattaforma SIDI e gestita in titolarità dal Ministero dell'Istruzione. In merito alla piattaforma G Suite for Education, ed in particolare Google Meet utilizzato per videoconferenza, è stato verificato il rispetto delle normative in materia di protezione dei dati personali da parte del fornitore. La Piattaforma Google Cloud Platform utilizza la crittografia come impostazione predefinita ed è applicata durante il transito dei dati tra il cliente e Google, nel caso di Meet, funziona interamente nel browser limitando l'esposizione ad eventuali attacchi informatici.

Il Registro Elettronico viene fornito da Axios Italia Service Srl con sede legale in Via E. Filiberto 190 - 00185 Roma (RM), P.IVA 06331261005, presenta garanzie sufficienti a mettere in atto misure tecniche e organizzative adeguate.

Non esistono processi decisionali automatizzati e non viene attuata una profilazione dei dati.

DIFFUSIONE, COMUNICAZIONE E SOGGETTI CHE ACCEDONO AI DATI

I dati personali forniti all'Istituto potranno essere comunicati al personale scolastico adeguatamente formato ed autorizzato per lo svolgimento delle attività educative ed amministrative ad esse connesse – ex art. 2-quaterdecies del d.lgs. 101/2018. Tali dati, inoltre, potranno risultare accessibili a soggetti esterni per finalità istituzionali o ad attività ed esse strumentali o per la fornitura dei servizi

necessari alla realizzazione delle attività educative ed amministrative, (ad es. società di servizio, fornitori di piattaforme e-learning o cloud, registro elettronico), questi soggetti sono nominati dal Titolare Responsabili del trattamento ai sensi dell'art. 28 del GDPR, inoltre, enti esterni che, a vario titolo possono effettuare attività di controllo/ispezione/verifica/audit, avendo come base di liceità l'obbligo legale/legittimo interesse/contratto. L'elenco dei soggetti esterni ed interni che possono accedere ai dati dell'Istituto, è disponibile facendone richiesta al Titolare, l'accesso a questi dati è subordinato alla valutazione della legittimità della richiesta.
Da ultimo, la comunicazione dei dati personali potrà essere effettuata verso enti e/o autorità pubbliche in base agli obblighi previsti dalla legge e/o da regolamenti, in particolare per la gestione di eventuali casi e focolai di SARS-CoV-2 nelle scuole, i dati verranno comunicati al Dipartimento di Prevenzione (DdP);

L'istituto non trasferisce dati personali in paesi terzi extra UE o ad organizzazioni internazionali, qualora ciò si rivelasse necessario ai fini istituzionali, per lo svolgimento delle attività educative, per la fruizione della Didattica Digitale Integrata, l'Istituto verificherà che sussistano tutti i presupposti giuridici per assicurare un adeguato livello di protezione.

DURATA DEL TRATTAMENTO E CONSERVAZIONE DEI DATI PERSONALI
Non è prevista la distruzione o cancellazione dai dati personali trattati nell'ambito dell'iscrizione ed eventuale conseguimento del titolo scolastico, salvo esplicita richiesta di cancellazione dei dati dell'interessato, che comunque saranno conservati solo per finalità espressamente previste dalla normativa di settore e per un periodo di tempo non superiore a quello a tali fini strettamente necessario allo svolgimento delle finalità istituzionali ed eventualmente in base alle scadenze previste dalle norme di legge. Microsoft assicura che tutte le copie dei dati personali sono eliminate entro 30 giorni successivi alla registrazione, inoltre, l'Istituto disporrà la cancellazione dei dati presso il fornitore al termine di specifici progetti didattici.

DIRITTI DELL'INTERESSATO
Contattando il Titolare, per tramite del Responsabile della Protezione dei Dati, l'interessato può esercitare i diritti previsti di cui agli artt. da 15 a 22 e per quanto applicabili in considerazione dell'art. 23 del Regolamento. Laddove richiesto, l'interessato ha il diritto di accesso ai propri dati personali, alla rettifica dei dati inesatti, alla cancellazione, alla limitazione o alla possibilità di opporsi al trattamento, di richiedere la portabilità dei dati, di revocare il consenso. La risposta alle richieste sarà fornita entro un mese, se la richiesta è troppo complessa o in presenza di numerose richieste tale periodo può prorogarsi di altri due mesi.
Inoltre, l'interessato ha sempre il diritto di proporre reclamo al Garante ai riferimenti presenti nel sito web: www.garanteprivacy.it, o di adire le opportune sedi giudiziarie.

Aggiornamento novembre 2022

IL DIRIGENTE SCOLASTICO
(Prof.ssa Patrizia Tozi)

CONSENSO AL TRATTAMENTO DEI DATI PERSONALI

Il/La sottoscritto/a .....

e Il/La sottoscritto/a .....

in qualità di: (specificare: genitore/tutore/delegato/responsabile genitoriale) .....

dell'alunno/a ..... iscritto/a alla classe ..... sezione .....

del plesso/della sede .....

preso atto delle presenti informazioni rese dal Titolare, ai sensi degli art. 13 del Regolamento, conferma di aver letto l'informativa completa sulla protezione dei dati personali trattati dall'Istituto ed esprime il suo consenso per le seguenti finalità:

Confermo di aver preso visione delle informazioni relative al trattamento dati personali di cui alla presente informativa	☐ Per presa visione
Per il trattamento dei dati per immagini all'interno delle attività educative e didattiche per scopi formativi e informativi.	☐ Presto il consenso ☐ Nego il consenso

Consapevole delle conseguenze civili e penali per chi rilasci dichiarazioni non corrispondenti a verità, ai sensi del DPR 245/2000, dichiara di aver effettuato la scelta del consenso in osservanza delle disposizioni sulla responsabilità genitoriale di cui agli artt, 316, 337 ter e 337 quater del Codice civile che richiedono il consenso di entrambi i genitori.

Roma, lì _____

Firma del primo genitore/tutore

_____

Firma del secondo genitore

_____

ALLEGATO 9: INFORMAZIONI AI FORNITORI DI BENI E SERVIZI, OPERATORI ECONOMICI ED ESPERTI ESTERNI

INFORMAZIONI AI FORNITORI DI BENI E SERVIZI, OPERATORI ECONOMICI ED ESPERTI ESTERNI ARTT. 13 E 14 DEL REGOLAMENTO EUROPEO N. 2016/679

Ai sensi e nel rispetto degli art. 13 e 14 del "*Regolamento Europeo 2016/679 relativo alla protezione delle persone fisiche con riguardo al Trattamento dei Dati Personali, nonché alla libera circolazione di tali dati*" (di seguito *GDPR*) e del D.Lgs..196/2003 e successive modifiche ed integrazioni, l'Istituto Comprensivo "Tullio De Mauro" Titolare del trattamento, nella persona del dirigente scolastico pro-tempore, al fine di garantire i diritti, le libertà fondamentali, nonché la dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale, pubblica nei modi e nei tempi previsti dalla normativa le presenti informazioni rivolte ai Fornitori di beni e servizi, operatori economici ed esperti esterni.

ESTREMI IDENTIFICATIVI DEL TITOLARE DEL TRATTAMENTO DATI PERSONALI

Il Titolare del Trattamento, (di seguito "Titolare") è l'Istituto Comprensivo Statale "Tullio De Mauro", con sede legale in Viale Fernando Santi, 65 - 00155 ROMA, nella persona del Dirigente Scolastico Prof.ssa Patrizia Tozi.
Dati di contatto: Tel. +39 06/ 95955067, E-mail: rmic8b5008@istruzione.it - PEC: rmic8b5008@pec.istruzione.it

RESPONSABILE PER LA PROTEZIONE DEI DATI PERSONALI

Ai sensi dell'art. 37 del Regolamento, il Titolare ha designato il Responsabile della Protezione dei Dati personali (RPD) o anche Data Protection Officer (DPO) nella persona di: Massimo Corinti
Dati di contatto: Mob. +39 335 7687380 - E-mail: dpo@corinti.eu - PEC: dpo@pec.corinti.eu.

CATEGORIE DI DATI PERSONALI TRATTATI DAL TITOLARE DEL TRATTAMENTO

Tutti i dati forniti, nell'ambito del rapporto con la presente istituzione scolastica, verranno trattati esclusivamente per le finalità istituzionali della scuola, che sono quelle relative all'istruzione ed alla formazione degli alunni e quelle amministrative ad esse strumentali, incluse le finalità relative alla conclusione di contratti di fornitura di beni e/o servizi e/o di concessione di beni e servizi, così come definite dalla normativa vigente (D.lgs. n. 297/1994, D.P.R. n. 275/1999; Decreto Interministeriale 1 febbraio 2001, n. 44 e le norme in materia di contabilità generale dello Stato; D.lgs. n. 165/2001, Legge 13 luglio 2015 n. 107, D.lgs.. 50/2016 e tutta la normativa e le prassi amministrative richiamate e collegate alle citate disposizioni).
Il conferimento dei dati richiesti è obbligatorio in quanto previsto dalla normativa sopra citata l'eventuale rifiuto a fornire tali dati potrebbe comportare il mancato perfezionamento o mantenimento del contratto.

FINALITÀ E BASI GIURIDICHE DEL TRATTAMENTO

Il trattamento dei suoi dati personali avrà le seguenti finalità:

- predisposizione e comunicazioni informative precontrattuali e istruttorie rispetto alla stipula del contratto;
- esecuzione del contratto e conseguente gestione amministrativa e contabile;
- adempimento di obblighi derivanti da leggi, contratti, regolamenti in materia di igiene e sicurezza del lavoro, in materia fiscale, in materia assicurativa;
- tutela dei diritti in sede giudiziaria.

MODALITA' DI TRATTAMENTO

I dati personali da Lei forniti, saranno trattati nel rispetto della normativa sopracitata e degli obblighi di riservatezza cui è ispirata l'attività del Titolare. I dati verranno trattati sia con strumenti informatici sia su supporti cartacei sia su ogni altro tipo di supporto idoneo, da soggetti autorizzati e adeguatamente formati, nel rispetto di adeguate misure tecniche ed organizzative di sicurezza previste dal GDPR.

DIFFUSIONE, COMUNICAZIONE E SOGGETTI CHE ACCEDONO AI DATI

La comunicazione/diffusione, in osservanza delle norme, riguarda i soli dati consentiti e per le sole finalità istituzionali obbligatorie.
I Suoi dati personali potranno essere comunicati a soggetti pubblici quali, ad esempio, Ministero dell'Istruzione e le sue articolazioni periferiche, altre Amministrazioni dello Stato ed enti preposti al rispetto delle norme su trasparenza, anticorruzione e antimafia (Prefettura, Questura, tribunali, ANAC, eccetera), nonché ad enti preposti alla verifica della sua regolarità fiscale (Agenzia delle Entrate, Equitalia, ecc.), sempre nei limiti di quanto previsto dalle vigenti disposizioni di legge e di regolamento e degli obblighi conseguenti per l'istituzione scolastica. Per eventuali ed esclusivi obblighi di legge, nei soli casi dovuti, i Suoi dati potranno essere diffusi mediante pubblicazione all'Albo e mediante altri mezzi di diffusione della Scuola (Sito Web e Amministrazione Trasparente).
I dati oggetto del trattamento, registrati in sistemi informativi cloud, sono conservati su server ubicati all'interno dell'Unione Europea e non sono oggetto di trasferimento.

DURATA DEL TRATTAMENTO E CONSERVAZIONE DEI DATI PERSONALI
Il Titolare tratterà i dati personali per il tempo necessario per adempiere alle finalità di cui sopra e comunque per non oltre 10 anni dalla cessazione del rapporto per le finalità di servizio. I tempi di conservazione sia cartacei che telematici sono stabiliti dalla normativa di riferimento per le Istituzioni scolastiche in materia di Archivistica.

DIRITTI DELL'INTERESSATO
Contattando il Titolare, o per tramite del Responsabile della Protezione dei Dati ai riferimenti di cui sopra, l'interessato può esercitare i diritti previsti dagli artt. 15 e ss. del Regolamento, e per quanto applicabili in considerazione dell'art. 23. Laddove richiesto, l'interessato ha il diritto di accesso ai propri dati personali, alla rettifica dei dati inesatti, alla cancellazione, alla limitazione o alla possibilità di opporsi al trattamento, di richiedere la portabilità dei dati, di revocare il consenso. La risposta alle richieste sarà fornita entro un mese, se la richiesta è troppo complessa o in presenza di numerose richieste tale periodo può prorogarsi di altri due mesi. Inoltre, l'interessato ha sempre il diritto di proporre reclamo all'Autorità Garante per la Protezione dei Dati Personali ai riferimenti presenti nel sito web: www.garanteprivacy.it come previsto dall'art. 77 del Regolamento, o di adire le opportune sedi giudiziarie ai sensi dell'art. 79 del Regolamento.

IL DIRIGENTE SCOLASTICO
(Prof.ssa Patrizia Tozi)

ALLEGATO 10: INFORMAZIONI AI FORNITORI DI BENI E SERVIZI - BANDO GARA

INFORMAZIONI SUL TRATTAMENTO DEI DATI PERSONALI
Art. 13 del Regolamento (UE) 2016/679

Ai sensi del Regolamento Generale dell'UE sulla Protezione dei Dati (RGPD o GDPR nel prosieguo "Regolamento") n. 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, considerando le disposizioni del d.lgs. 196/2003 e s.m.i. c.d. "Codice privacy", come novellato dal d.lgs. 101/2018, la informiamo che i dati personali forniti all'Istituto Comprensivo Statale "Tullio De Mauro", saranno trattati secondo i principi di liceità, correttezza e trasparenza al fine di garantire i diritti, le libertà fondamentali, nonché la dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale.

ESTREMI IDENTIFICATIVI DEL TITOLARE DEL TRATTAMENTO DATI PERSONALI
Il Titolare del Trattamento, (di seguito "Titolare") è l'Istituto Comprensivo Statale "Tullio De Mauro", con sede legale in Viale Fernando Santi, 65 - 00155 ROMA, nella persona del Dirigente Scolastico Prof.ssa Patrizia Tozi.
Dati di contatto: Tel. +39 06/ 95955067, E-mail: rmic8b5008@istruzione.it - PEC: rmic8b5008@pec.istruzione.it

RESPONSABILE PER LA PROTEZIONE DEI DATI PERSONALI
Ai sensi dell'art. 37 del Regolamento, il Titolare ha designato il Responsabile della Protezione dei Dati personali (RPD) o anche Data Protection Officer (DPO) nella persona di: Massimo Corinti
Dati di contatto: Mob. +39 335 7687380 - E-mail: dpo@corinti.eu - PEC: dpo@pec.corinti.eu

CATEGORIE DI DATI PERSONALI TRATTATI DAL TITOLARE DEL TRATTAMENTO
In relazione alle attività relative alla fornitura di beni e/o servizi il Titolare informa che i dati personali dell'interessato, nel caso in cui sia una persona fisica o una ditta individuale, di seguito il "Fornitore", dei suoi dipendenti o incaricati, comunicati per l'acquisizione e selezione dello stesso alle procedure di gara, nel corso dell'esecuzione del rapporto contrattuale e per te le attività ad esso connesse tra il Titolare e il fornitore, potranno essere trattati dati nei quali rientrano le generalità, l'anagrafica completa, inclusi eventuali numeri di identificazione personale, recapiti quali per es. numero di cellulare, indirizzo e-mail, tali dati saranno trattati in conformità dei principi di previsti dal Regolamento.

FINALITÀ E BASI GIURIDICHE DEL TRATTAMENTO
I dati personali raccolti saranno trattati, senza previo consenso da parte dell'interessato, per le seguenti finalità:
a) l'esecuzione del contratto e/o di impegni precontrattuali:
   - la gestione dei rapporti precontrattuali e contrattuali;
   - l'esecuzione del contratto;
   - la gestione degli incassi e dei pagamenti.
b) il perseguimento di un legittimo interesse del Titolare:
   - l'esercizio dei diritti del Titolare in sede giudiziaria e la gestione degli eventuali contenziosi;
   - la prevenzione e repressione di atti illeciti.
c) l'adempimento di obblighi di legge:
   - la tenuta della contabilità e degli adempimenti ad essa relativi;
   - la compilazione ed elaborazione delle dichiarazioni fiscali e degli adempimenti alle stesse connesse;

- l'ottemperanza agli obblighi previsti da leggi, regolamenti o dalla normativa comunitaria ovvero imposti dalle Autorità, ivi compresa l'esecuzione di comunicazioni alle autorità competenti e agli organi di vigilanza e per conformarsi con richieste provenienti dalle stesse.

Il rifiuto di fornire i dati per le finalità di cui alle lettere da a) a c) sopra indicate avrebbe il risultato di impedire al Titolare di concludere il Contratto, e se già concluso, di proseguirne l'esecuzione.

TRATTAMENTI AUTOMATIZZATI
Non esistono processi decisionali automatizzati e non viene attuata una profilazione dei dati.

MODALITA' DI TRATTAMENTO
I dati personali da Lei forniti, saranno trattati nel rispetto della normativa sopracitata e degli obblighi di riservatezza cui è ispirata l'attività del Titolare. I dati verranno trattati sia con strumenti informatici sia su supporti cartacei sia su ogni altro tipo di supporto idoneo, da soggetti autorizzati e adeguatamente formati, nel rispetto delle misure previste dal GDPR.

DIFFUSIONE, COMUNICAZIONE E SOGGETTI CHE ACCEDONO AI DATI
Per tutta la durata del trattamento il Titolare garantirà l'integrità e la riservatezza dei dati personali che saranno trattati dai soli soggetti autorizzati dal Titolare riconducibili alle seguenti categorie:

a) persone fisiche autorizzate e nominate dal Titolare al trattamento di dati personali ex art. 29 GDPR in ragione dell'espletamento delle loro mansioni lavorative quali:
b) collaboratori, dipendenti e fornitori del Titolare, nell'ambito delle relative mansioni e/o di eventuali obblighi contrattuali.
c) fornitori di servizi i quali agiscono tipicamente in qualità di responsabili del trattamento ex art. 28 del Regolamento quali:
   - consulenti legali, amministrativi e fiscali che assistono il Titolare nello svolgimento delle attività;
   - subfornitori e/o subappaltatori impegnati in attività connesse all'esecuzione del Contratto con il Titolare
   - fornitori di servizi cloud o IT;
d) istituti bancari per la gestione d'incassi e pagamenti derivanti dall'esecuzione del Contratto con il Fornitore;

L'elenco completo ed aggiornato dei destinatari dei dati potrà essere richiesto al Titolare, ai recapiti sopra indicati.
L'istituto non trasferisce dati personali in paesi terzi o organizzazioni internazionali, qualora ciò si rivelasse necessario provvederemo ad informarla.

DURATA DEL TRATTAMENTO E CONSERVAZIONE DEI DATI PERSONALI
Il Titolare tratterà i dati personali per il tempo necessario per adempiere alle finalità di cui sopra e comunque non oltre 10 anni dalla cessazione del rapporto contrattuale.

DIRITTI DELL'INTERESSATO
Contattando il Titolare, o per tramite del Responsabile della Protezione dei Dati ai riferimenti di cui sopra, l'interessato può esercitare i diritti previsti dagli artt. 15 e ss. del Regolamento, e per quanto applicabili in considerazione dell'art. 23. Laddove richiesto, l'interessato ha il diritto di accesso ai propri dati personali, alla rettifica dei dati inesatti, alla cancellazione, alla limitazione o alla possibilità di opporsi al trattamento, di richiedere la portabilità dei dati, di revocare il consenso. La risposta alle richieste sarà fornita entro un mese, se la richiesta è troppo complessa o in presenza di numerose richieste tale periodo può prorogarsi di altri due mesi. Inoltre, l'interessato ha sempre il diritto di proporre reclamo all'Autorità Garante per la Protezione dei Dati Personali ai riferimenti presenti nel sito web: www.garanteprivacy.it come previsto dall'art. 77 del Regolamento, o di adire le opportune sedi giudiziarie ai sensi dell'art. 79 del Regolamento.

ALLEGATO 11: CONSENSO INFORMATO - LIBERATORIA

CONSENSO INFORMATO PER GENITORI/TUTORE LEGALE – (BOZZA DA VERIFICARE CON IL DPO)
Ex Art. 13 del Regolamento (UE) 2016/679

Ai sensi del Regolamento Generale dell'UE sulla Protezione dei Dati n. 2016/679, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati considerando le disposizioni del d.lgs. 196/2003 e s.m.i. cd. "Codice privacy", la informiamo che nell'abito _____ l'Istituto Comprensivo "Tullio De Mauro" _____: _____, per _____scopi esclusivamente _____ verranno effettuate riprese audio-video.
Il Dirigente scolastico assicura che le riprese audio-video non consentiranno l'identificazione univoca dell'alunno, inoltre, assicura che non verranno trattati dati personali per il trattamento di cui sopra:

Io sottoscritta (madre/tutore) _____

Io sottoscritto (padre/tutore) _____

GENITORI/TUTORI LEGALI

Dell'alunno _____

dichiarano di aver ricevuto completa Informativa ai sensi dell'art. 13 del Regolamento europeo 679/2016 in materia di protezione dei dati personali, dichiarano altresì di essere nel pieno possesso dei diritti di esercizio della potestà genitoriale/tutoria nei confronti del minore, autorizzano il trattamento per le riprese audio-video.

_____	__/__/_____	_____
genitore/tutore legale	Data	Firma
_____	__/__/_____	_____
genitore/tutore legale	Data	Firma

Roma, lì

ALLEGATO 13: ANALISI DEI RISCHI PRIVACY

Da valutare