ISTITUTO COMPRENSIVO "RINNOVATA PIZZIGONI" Via Castellino da Castello, 10 Milano (MI)

Modello Organizzativo sul Trattamento dei Dati Regolamento Europeo Privacy 679/2016

SOMMARIO

ATTENZIONE! Prima di utilizzare il presente documento verificare che sia in ultima edizione

Revisioni e/o aggiornamenti

Ed.	Data	Descrizione revisione e/o aggiornamento
01	20 Novembre 2019	Redatto documento programmatico sulla sicurezza dei dati personali in ottemperanza al Regolamento Europeo 679/2016
02	04 Settembre 2020	Aggiornato documento programmatico sulla sicurezza dei dati personali in ottemperanza al Regolamento Europeo 679/2016

1 SCOPO

1.1 Premessa

Il presente documento è stato redatto in conformità al Regolamento Generale dell'Unione Europea sulla protezione dei dati, 27 Aprile 2016, n. 679 (GDPR 679/2016), al fine di individuare, analizzare ed applicare un complesso di contromisure per garantire la massima sicurezza in ordine al trattamento dei dati personali.
Tale documento viene aggiornato con frequenza annuale.
L'Istituto Comprensivo "Rinnovata Pizzigoni" di Milano (di seguito "IC Rinnovata Pizzigoni") effettua un'attività di informativa nei confronti del personale, dei collaboratori e degli allievi e delle loro famiglie.

1.2 Finalità

Il presente documento ha lo scopo di:

- Definire e riportare sotto il profilo normativo gli obblighi che l'IC RINNOVATA PIZZIGONI deve adempiere in merito all'adozione delle misure minime di sicurezza.
- Tutelare gli interessi dei soggetti pubblici e privati che fanno affidamento sui trattamenti di dati personali svolti dall'Istituto.
- Evitare eventi pregiudizievoli che possono danneggiare disponibilità, riservatezza e integrità del patrimonio dati personali trattati dall'IC RINNOVATA PIZZIGONI.
- Potenziare la consapevolezza dei rischi e delle insidie che possono coinvolgere il trattamento dei dati personali effettuato con l'ausilio di sistemi informativi automatizzati o tramite supporto cartaceo.
- Definire le soluzioni logiche, fisiche e organizzative al fine di prevenire situazioni di pericolo.
- Individuare le misure di sicurezza e le procedure per ridurre al minimo la distruzione o la perdita dei dati, l'accesso non autorizzato ed il trattamento non consentito o non conforme.

2 PRINCIPI GENERALI APPICABILI AL TRATTAMENTO DEI DATI PERSONALI

Si riportano i principi generali alla base del trattamento dei dati personali, adottati dall'IC RINNOVATA PIZZIGONI. I dati personali sono:

a) Trattati in modo lecito, corretto e trasparente nei confronti dell'interessato: principio di "*liceità*, *correttezza* e *trasparenza*".

b) Raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali principio di "*limitazione della finalità*".

c) Adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati: principio di "*minimizzazione dei dati*".

d) Esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati: principio di "*esattezza*".

e) Conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato: principio di "*limitazione della conservazione*".

f) Trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali: principio di "*integrità e riservatezza*".

2.1 Il principio di "Accountability" - Responsabilizzazione

L'IC RINNOVATA PIZZIGONI, in qualità di Titolare del trattamento, si impegna ad adottare politiche ed attuare misure adeguate al fine di garantire ed essere in grado di dimostrare che il trattamento dei dati personali effettuato è conforme alle disposizioni del GDPR 679/2016.

3 CAMPO DI APPLICAZIONE

Il presente documento definisce le politiche e gli standard di sicurezza in merito al trattamento, interamente o parzialmente automatizzato, di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi, in particolare:

- l'analisi dei trattamenti di dati personali;
- la distribuzione dei compiti e delle responsabilità;
- l'analisi dei rischi che incombono sui dati in termini di impatto;
- le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali rilevanti ai fini della loro custodia e accessibilità;
- la descrizione dei criteri e delle modalità di ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento;
- la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati;
- la definizione di idonee misure di sicurezza in caso di trattamenti effettuati da parte di soggetti esterni.

4 RIFERIMENTI NORMATIVI

- D. Lgs. 196 del 30 giugno 2003 "*Codice in materia di Protezione dei dati personali - Legge delega n. 127/2001*" e ss.mm.ii come novellato dal D. Lgs. 101 del 10 agosto 2018 "*Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE*".
- Provvedimento del Garante del 27 novembre 2008 "*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema*".
- Provvedimento del Garante del 13 ottobre 2008 "*Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali*" .
- Decreto Legge 6/12/2011 n. 201 che all'art. 4 modifica l'ambito di applicazione del Codice Privacy, ora allineato a quanto previsto dalla normativa europea.
- D. Lgs. 28 maggio 2012, n. 69 in attuazione alla delega prevista nell'art. 9 della Legge comunitaria del 2010 (L. n. 217/2011) per il recepimento della direttiva 2009/136/CE in materia di trattamento dei dati personali e tutela della vita privata nel settore delle comunicazioni elettroniche.
- Provvedimento del Garante 08/05/2014 n° 229 "*Individuazione delle modalità semplificate per l'informativa e l'acquisizione del consenso per l'uso dei cookie*".
- Regolamento Europeo 2016/679 in materia di Protezione dei Dati Personali.
- DPCM 11 marzo 2020, in particolare Protocollo Condiviso 14 marzo 2020, Protocollo 24 aprile 2020 e successive integrazione e modificazioni nell'ambito dell'emergenza COVID

4.1 Riferimenti bibliografici

- ENISA "Handbook on Security of Personal Data Processing"
- CNIL-PIA Methodology
- Metodologia VERA Privacy – Cesare Gallotti
- AgID Basic Security Control

5 DEFINIZIONI

a) **"Trattamento**": qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insieme 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.

b) **"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 online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

c) **"Categorie particolari di dati":** i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale (anche indicati come dati sensibili nel presente documento).

d) **"Limitazione di trattamento":** il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro.

e) **"Profilazione":** qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di 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.

f) **"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 organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.

g) **"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.

h) **"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.

i) **"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.

j) **"Destinatario":** la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di tali 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.

k) **"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.

l) **"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.

m) **"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.

n) **"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.

o) **"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.

p) **"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.

q) **"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 presente regolamento.

r) **"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 presente regolamento.

s) **"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.

t) **"Gruppo imprenditoriale":** un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate.

u) **"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.

v) **"Autorità di controllo":** l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51.

w) **"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.
- Gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure
- Un reclamo è stato proposto a tale autorità di controllo.

x) **"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 del trattamento o Responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro.

y) **"Obiezione pertinente e motivata"**: un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente regolamento, oppure che l'azione prevista in relazione al Titolare del trattamento o Responsabile del trattamento sia conforme al presente regolamento, 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.

z) **"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.

aa) **"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.

bb) **"Interessato"**: La definizione di "interessato", non essendocene una diretta, è desumibile dall'articolo 5, comma 1 che, definendo il "dato personale" dispone che: "*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 online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale*".

6 ANALISI DEL CONTESTO IN CUI OPERA L'ISTITUTO E PARTI INTERESSATE

L'IC RINNOVATA PIZZIGONI è un Istituto Comprensivo scolastico con sede amministrativa principale situata in Via Castellino da Castello, 10 a Milano (MI).

L'Istituto risulta essere composto dai seguenti plessi:
- Scuola Primaria "Rinnovata Pizzigoni";
- Scuola Primaria "Dante Alighieri";
- Scuola Secondaria I grado "Giancarlo Puecher".

La Scuola accoglie circa 1250 alunni minorenni. Il personale conta in totale circa 150 unità del corpo docente, 30 del personale di segreteria e collaboratori scolastici, il Direttore Amministrativo (DSGA).

6.1 Descrizione del processo produttivo

L'IC RINNOVATA PIZZIGONI offre il servizio di istruzione scolastica pubblica, con particolare differenziazione del metodo didattico impartito. L'Istituto, infatti, abbraccia il "metodo Pizzigoni", consistente nell'osservazione derivante da attività pratiche per condurre successivamente lo studente a dedurre la teoria. Per tali scopi didattici, gli spazi scolastici comprendono una piccola azienda zootecnica, un orto a terra, una piscina, spazi laboratoriali integrati e aule all'aperto.
La Scuola effettua il trattamento di dati personali e appartenenti a categorie particolari con riferimento al personale docente e ATA per finalità connesse alla gestione del rapporto lavorativo e degli aspetti relativi alla salute e alla sicurezza sui luoghi di lavoro.
L'Istituto tratta le stesse categorie di dati relativi agli alunni iscritti e alle loro famiglie per finalità legate all'erogazione del servizio di istruzione, alla salute e alla sicurezza sui luoghi scolastici, alla gestione di dati provenienti da fotografie, audio e filmati, al servizio mensa e all'utilizzo della piattaforma digitale.
Ulteriori dati personali vengono trattati in occasione della gestione delle Messe a disposizione (MAD) e degli incarichi a collaboratori, professionisti esterni e consulenti che svolgano attività all'interno dell'Istituto.
L'IC RINNOVATA PIZZIGONI utilizza un sito internet a fini istituzionali; a breve sarà implementata e disponibile anche una pagina Facebook. Sul sito sono presenti i collegamenti ad altre piattaforme ufficiali, quali "Puecher Monitor", "Puecher Inside", "Voices", AGIR (Associazione Genitori) e Opera Pizzigoni.
Non è presente un sistema di videosorveglianza.
Nello svolgimento di alcune attività sopra menzionate, l'Istituto si avvale di professionisti esterni ai quali affida, totalmente o in parte, la gestione dei relativi servizi; qualora sia necessario il trattamento di dati personali per tali finalità, l'Istituto provvede a nominare il fornitore quale Responsabile esterno del trattamento.

Eventuale rilevazione della temperatura in ingresso e la gestione degli accessi per il personale interno o esterno è effettuata secondo quanto previsto dal Protocollo Aziendale predisposto in conformità al DPCM 11 marzo 2020, in particolare Protocollo Condiviso 14 marzo 2020, Protocollo 24 aprile 2020 e successive integrazione e modificazioni.

Nell'ambito dell'emergenza COVID19 è stato applicato un protocollo sulla salute e sicurezza che prevede misure organizzative e di protezione dei dipendenti, relativamente a:

- informazione ai lavoratori sulle condizioni che precludono l'accesso in azienda (al fine di minimizzare il rischio di contagio e il trattamento dei dati personali)
- modalità di accesso agli uffici
- utilizzo di procedure dedicate per la pulizia e la sanificazione dei locali
- adozione di DPI e procedure per il personale che accede agli uffici

- organizzazione del lavoro, inclusa la gestione degli spazi comuni,riunioni
- gestione delle persone sintomatiche
- gestione di eventuali lavoratori fragili, a cura del Medico Competente

Nell'ambito delle misure organizzative previste è stata adottata la modalità di lavoro in smartworking. I dipendenti utilizzano i dispositivi aziendali o eventuali dispostivi personali secondo quando definito nel Regolamento aziendale per l'utilizzo di sistemi informativi.

6.2 Infrastruttura HW – SW

Il sistema informativo dell'IC RINNOVATA PIZZIGONI è costituito dalla presenza di computer client in rete tra di loro protetti da una password associata a ciascun utente.
Sono presenti due differenti reti scolastiche separate relative alla segreteria e alla didattica. La rete di segreteria è presente esclusivamente presso la sede di Via Castellino da Castello, 10.
Per quanto concerne i software è il Titolare del trattamento che definisce i software standard scolastici.

È vietato, per l'utente, installare software di qualsiasi tipo, scaricato da Internet, giochi, screen saver o qualsiasi altra utility non preventivamente autorizzata dall'IC RINNOVATA PIZZIGONI. È necessario attenersi ai software ufficiali per evitare i rischi di infezione da virus e problemi di conflitto tra software.

Si riporta la configurazione software di base dei pc.

NOME SOFTWARE	DESCRIZIONE	UTILIZZATORI
Windows 7	Sistemi Operativi	Tutti gli autorizzati – su pc
Microsoft Office	Software Gestionale	Tutti gli autorizzati – su pc
	Antivirus	Tutti gli autorizzati – su server e pc
Axios	Gestionale area amministrativa e contabile Segreteria digitale Gestionale registro elettronico	Tutti gli autorizzati tramite credenziali personali – su server, pc e gestionale
Host S.p.A.	Hosting sito internet	Autorizzati alla gestione del sito – su web hosting
Aruba	Dominio email	Tutti gli autorizzati tramite credenziali personali – su server e pc

Si riporta la configurazione dei dispostivi hardware

NOME HARDWARE	NUMERO	UTILIZZATORI
Computer fissi	9	Tutti gli autorizzati tramite credenziali individuali
Laboratori informatici	2	Personale docente e alunni
Stampanti / fotocopiatrici	4	Tutti gli autorizzati tramite credenziali individuali

Server	1	Direzione Amministratore di Sistema Tramite credenziali
Firewall	1	Amministratore di Sistema

6.3 Sito internet

L'IC RINNOVATA PIZZIGONI utilizza un sito internet (www.scuolarinnovata.it) a fini istituzionali per presentare e illustrare le attività scolastiche e i servizi offerti, mostrare gli eventi, i contatti e la posizione geografica.
Nel sito potrebbero essere presenti immagini che raffigurano il personale dipendente e gli allievi; per tale pubblicazione sono stati resi specifici consensi e liberatorie da parte dell'Istituto.
Il sito raccoglie cookies di tipo tecnico, non di profilazione. Al primo accesso al sito compare il relativo banner informativo.
L'Istituto a breve implementerà una pagina Facebook. Inoltre, sul sito sono presenti i collegamenti ad altre piattaforme ufficiali, quali "Puecher Monitor", "Puecher Inside", "Voices", AGIR (Associazione Genitori) e Opera Pizzigoni.

6.4 Videosorveglianza

L'IC RINNOVATA PIZZIGONI non è dotato di un impianto di videosorveglianza.

Finalità del trattamento o attività svolta Interessati: DIPENDENTI	Tipologia trattamento	Base giuridica trattamento	Soggetti incaricati	Soggetti esterni che effettuano il trattamento	Tempo di conservazione	Strumenti e banche dati utilizzati
Prevenzione dal COVID-19 Tutela della salute Collaborazione con le autorità pubbliche	Temperatura corporea senza registrazione	DPCM 11/03/20 Protocollo Condiviso 14/03/20 – 24/04/20	Incaricati all'ingresso (solo se previsto)	--	Nessuna registrazione	Termometri
	Dati identificativi del superamento soglia di 37,5°- sintomi - zone a rischio, contatti stretti	DPCM 11/03/20 Protocollo Condiviso 14/03/20 – 24/04/20	Incaricati all'ingresso (solo se previsto)	Incaricati Area Amministrazione	Solo se necessario fino al termine dell'emergenza	Comunicazione all'ufficio personale
	Stato di salute (eventuale negativizzazione del tampone)	DPCM 11/03/20 Protocollo Condiviso 14/03/20 – 24/04/20	--	Medico Competente	Fino al termine dell'emergenza o comunicazioni delle autorità	Cartella sanitaria del dipendente
	Presenza di stato di fragilità (lavoratori fragili)	DPCM 11/03/20 Protocollo Condiviso 14/03/20 – 24/04/20	--	Medico Competente	Fino al termine dell'emergenza o comunicazioni delle autorità	Cartella sanitaria del dipendente

Finalità del trattamento o attività svolta Interessati: COLLABORATORI O VISITATORI	Tipologia trattamento	Base giuridica trattamento	Soggetti incaricati	Soggetti esterni che effettuano il trattamento	Tempo di conservazione	Strumenti e banche dati utilizzati
Gestione emergenza Covid-19	Temperatura corporea senza registrazione	DPCM 11/03/20 Protocollo Condiviso 14/03/20 24/04/20 e successive integrazioni	Incaricati	--	Nessuna registrazione	Termometri
	Registrazione dei dati anagrafici (nome, cognome, data di nascita, luogo di residenza), dei relativi recapiti telefonici, nonché della data di accesso e del tempo di permanenza nell'Istituto	DPCM 11/03/20 Protocollo Condiviso 14/03/20 24/04/20 e successive integrazioni	Incaricati all'ingresso	Incaricati	Fino al termine dello stato d'emergenza dell'emergenza	Registro cartaceo

Finalità del trattamento o attività svolta Interessati:Alunni	Tipologia trattamento	Base giuridica trattamento	Soggetti incaricati	Soggetti esterni che effettuano il trattamento	Tempo di conservazione	Strumenti e banche dati utilizzati
Emergenza Covid-19 Dati sanitari relativi ad una particolare situazione di fragilità in cui versa lo studente, determinata dalle specifiche patologie di cui sia eventualmente affetto; Per gli studenti risultati positivi al COVID-19, ai fini del rientro a scuola, certificazione medica da cui risulti la "avvenuta negativizzazione" del tampone secondo le modalità previste e rilasciata dal dipartimento di prevenzione territoriale di competenza.	Dati sanitari	Obblighi di legge	Incaricati	--	Fino al termine dello stato d'emergenza	Strumenti cartacei o informatici

7 ANALISI DEI DATI PERSONALI TRATTATI

L'IC RINNOVATA PIZZIGONI tratta i dati personali per i seguenti scopi:

a) gestione delle Risorse Umane (attività svolte per la gestione della forza lavoro dell'Istituto, come l'assunzione, la retribuzione, il percorso professionale, la valutazione, formazione, il rispetto della Legge applicabile, le comunicazioni al personale e/o alle loro rappresentanze);

b) esecuzione e gestione organizzativa e operativa delle attività scolastiche necessarie per garantire l'operatività dell'Istituto, come la programmazione del lavoro e la gestione delle risorse della Scuola;

c) adozione di quanto previsto dalla normativa vigente in materia di Salute e Sicurezza sul lavoro, comprese tutte le attività necessarie a garantire la sicurezza dei lavoratori, incluse le attività relative alla Medicina del Lavoro.

d) gestione ed organizzazione della composizione delle classi di studenti e delle attività connesse all'istruzione e alla didattica;

e) gestione del servizio di ristorazione scolastica;

f) gestione ed organizzazione degli organi collegiali e delle loro adunanze.

7.1 Categorie dei dati personali trattati e di interessati

La natura dei dati trattati è stata classificata sulla base di quanto previsto dal Regolamento Europeo 679/2016. Nello specifico, si è proceduto alla verifica ed alla successiva categorizzazione dei dati per tipologia. In particolare i dati più rilevanti trattati dal Titolare del trattamento sono:

a) Dati relativi alle Risorse Umane, di natura potenzialmente anche sensibile. A tal proposito si segnala che il Titolare del trattamento, al quale sono fornite informazioni di carattere personale strettamente indispensabili per dare esecuzione al rapporto di lavoro, individua il personale che può trattare tali dati e assicura idonee misure di sicurezza per proteggerli da indebite intrusioni o illecite divulgazioni.

b) Dati personali che si riferiscono a persone fisiche nell'ambito dei rapporti tra l'Istituto e gli studenti, i docenti, il personale dipendente e collaboratore.

c) Dati personali relativi ad altri soggetti (candidati all'assunzione, consulenti e professionisti, agenti nel caso in cui il trattamento riguardi dati ulteriori rispetto a quelli meramente scolastici).

d) Dati relativi alle Risorse Umane, di natura potenzialmente anche sensibile. A tal proposito si segnala che il Titolare del trattamento, al quale sono fornite informazioni di carattere personale strettamente indispensabili per dare esecuzione al rapporto di lavoro, individua il personale che può trattare tali dati e assicura idonee misure di sicurezza per proteggerli da indebite intrusioni o illecite divulgazioni.

e) Dati giudiziari relativi al personale che instaura rapporti con gli allievi.

Si riporta la sintesi delle categorie di dati personali trattati dall'IC RINNOVATA PIZZIGONI

Tipologia	Descrizione	Applicato
Identificativi	- Nome, Cognome, sesso, indirizzo istituzionale, telefono istituzionale, email istituzionale	☑
Altri dati identificativi	- Età, luogo e data di nascita, indirizzo privato, numero di telefono privato, email personale. - Numero di carta identità/numero di passaporto - Dati fisici (altezza, peso) - Auto aziendale (modello e targa) - Codice fiscale - Carte sanitarie - Stato civile, figli, soggetti a carico, appartenenti al nucleo familiare	☑ ☑ ☑ ☑ ☐ ☑ ☑ ☑
Immagini	- Immagini e filmati - Immagini o suoni raccolti dall'impianto di videosorveglianza	☑ ☐
Categorie particolari	- Dati idonei a rilevare lo stato di salute - Dati idonei a rivelare lo stato di gravidanza. - Dati idonei a rivelare l'appartenenza a categorie protette. - Dati idonei a rivelare lo stato di disabilità. - Origini razziali o etniche - Appartenenza religiosa - Appartenenza ad associazioni sindacali - Giudizi di idoneità alla mansione in caso di restrizioni - Infortuni, informazioni raccolte nell'ambito di quanto definito dalla normativa in materia di Salute e Sicurezza sul lavoro	☑ ☑ ☑ ☑ ☑ ☑ ☑ ☑ ☑
Dati giudiziari	- Carichi pendenti - Casellario giudiziale	☑ ☑
Istruzione e cultura	- Curriculum di studi e/o accademico. - Titoli di studio - Pubblicazioni e lavori attribuibili all'interessato	☑ ☑ ☑
Esperienze Lavoro	- Occupazione attuale e precedente. - Informazioni sul tirocinio o sulla formazione professionale. - Dati relativi alle pregresse esperienze professionali. - Retribuzioni, assegni, integrazioni salariali e trattenute.	☑ ☑ ☑ ☑
Dati commerciali e finanziari	- Dati contabili - Ordini, fatture, contratti - Transazioni - Identificativi finanziari - Dati finanziari relativi a investimenti, passività, solvibilità, prestiti, mutui, ipoteche, crediti, indennità, benefici, concessioni, donazioni, sussidi, contributi - Dati assicurativi - Dati previdenziali	☑ ☑ ☑ ☑ ☐ ☐ ☑ ☑
Profilazione	- Acquisti effettuati, servizi ricevuti, preferenze espresse, cookies - Carte fedeltà	☐ ☐
Dati di navigazione	- Profili utenti (dati di navigazione) Preferenze di navigazione	☑ ☐
Geolocalizzazione e controllo accessi	- Strumenti di rilevazione presenze (es. registrazione di ingressi o uscite presso luoghi di lavoro tramite badge o codici personali) - Geolocalizzazione di veicoli - Geolocalizzazione effettuata attraverso dispositivi mobili	☑ ☐ ☐
Dati biometrici	- Dati identificativi per rilevazione presenze o gestione accessi ai luoghi scolastici	☐
Abitudini di vita e consumo	- Viaggi, spostamenti, preferenze o esigenze alimentari - ad eccezione di quelle fondate su convinzioni religiose o filosofiche - Dati relativi all'appartenenza ad associazioni diverse da quelle di carattere religioso, filosofico, politico o sindacale, (es. licenze, autorizzazioni, dati relativi ad attività sportive o agonistiche)	☐ ☐

Il dettaglio dei trattamenti è riportato nel Registro delle attività di trattamento allegato al presente documento.

8 INDIVIDUAZIONE FIGURE E COMPITI

8.1 Titolare del trattamento

Ai sensi del Regolamento Europeo 2016/ si intende per 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*".

Il Titolare del trattamento deve assolvere a tutta una serie di obblighi così come previsto dall'articolo 30 del Regolamento Europeo 679/2016 a cui si rimanda.

Il Titolare del trattamento è l'IC RINNOVATA PIZZIGONI nella persona del Dirigente Scolastico pro tempore.

Il Titolare del trattamento ha individuato nella figura del DSGA il Referente Privacy nell'ambito dei trattamenti effettuati dagli incaricati.

8.2 Responsabile del trattamento - esterno

Per Responsabile del trattamento si intende "*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento*".

Il Responsabile del trattamento deve presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento dei dati personali garantisca la tutela dei diritti dell'interessato.

I compiti del Responsabile del trattamento sono individuati all'articolo 28 del Regolamento Europeo 2016/679.

I Responsabili del trattamento esterni che trattano dati per conto dell'IC RINNOVATA PIZZIGONI sono i seguenti:

Nominativo Responsabile	Attività svolta	Tipologia di trattamento
(in fase di assegnazione)	Medicina del lavoro	Dati personali e categorie particolari
Nuovo Studio Associato 626	RSPP - Sicurezza	Dati personali
Axios Service Italia S.r.l.	Fornitura gestionale amministrazione e segreteria Fornitura registro elettronico	Dati personali e categorie particolari
Milano Ristorazione	Servizio ristorazione	Dati personali e categorie particolari
Anvis Service s.n.c.	Gestione IT / AdS	Dati personali e categorie particolari
Host S.p.A.	Hosting sito internet	Dati personali
Società Assicurativa	Gestione polizze scolastiche	Dati personali
Professionisti esterni Cooperative Cresco e Aias	Attività didattiche ed extra-didattiche svolte presso l'Istituto	Dati personali e/o categorie particolari

8.3 Responsabile della protezione dei dati (DPO)

Secondo il Regolamento Europeo 2016/679 l'istituzione del DPO è obbligatoria nei seguenti casi:

a) Il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali.

b) Le attività principali del Titolare del trattamento o del Responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala.

c) Le attività principali del Titolare del trattamento o del Responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10.

Nell'articolo 5 del Regolamento UE 2016/679, che offre le definizioni, ne manca una specifica di Responsabile della protezione dei dati. Il profilo è desunto dall'articolo 37, che al comma 5 dispone che "*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 delle capacità di assolvere i compiti di cui all'articolo 39*".

L'articolo 39, per l'appunto, individua i compiti del DPO:

- 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 Regolamento UE 679/2016 nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati.
- Sorvegliare l'osservanza del Regolamento UE 679/2016, di altre disposizioni dell'Unione o degli Stati membri 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.
- Fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento.
- Cooperare con l'autorità di controllo.
- Fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento.

Tutto ciò premesso, l'IC RINNOVATA PIZZIGONI ha individuato come Responsabile della Protezione dei dati personali la Società Frareg S.r.l. nella persona dell'Ing. Stéphane Barbosa e ne ha fatto comunicazione al Garante per la Protezione dei Dati Personali. I dati di contatto sono pubblicati sul sito dell'Istituto e all'interno delle informative.

8.4 Amministratore di sistema

È stato individuato un tecnico della Società Anvis Service s.n.c. in qualità di Amministratore di Sistema, che sarà incaricato di espletare i seguenti compiti:

- supportare il DPO nel definire le misure di sicurezza informatica da adottare e supervisionare e/o provvedere in prima persona alla loro attuazione;
- monitorare il corretto funzionamento della rete, compresa la gestione dei filtri e del firewall;
- gestire e monitorare il sistema di backup;
- predisporre, per ogni incaricato del trattamento, delle credenziali di accesso;
- revocare tempestiva di tutti i profili di identificazione e gli account di posta su comunicazione scritta del Titolare del trattamento;
- segnalazione al Titolare del trattamento sulle non corrispondenze con le norme di sicurezza e su eventuali anomalie.

La nomina dell'Amministratore di Sistema è conservata in allegato al presente documento.
Sul server è presente un sistema di tracciamento che permette di memorizzare gli accessi al server. Il sistema garantisce la inalterabilità della registrazione degli accessi.

8.5 Incaricati del trattamento

Per incaricato del trattamento si intende "*la persona fisica autorizzata a compiere operazioni di trattamento dal Titolare o dal Responsabile*".

L'articolo 29 del Regolamento UE 2016/679 dispone che "*il Responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del Titolare del trattamento, che abbia accesso ai dati personali non può trattare tali dati se non è istruito in tal senso dal Titolare del trattamento*".

Pertanto, al fine di svolgere le attività di trattamento dei dati personali, occorre essere espressamente autorizzati in qualità di incaricato del trattamento.

Tutto ciò comporta che, ogni persona fisica, che operi in nome e/o nell'interesse dell'IC RINNOVATA PIZZIGONI e che per questo abbia bisogno di accedere ai dati trattati dall'Istituto, deve essere individuata in qualità di incaricato e conseguentemente essere autorizzata ad accedere ai dati, di cui è Titolare la Scuola medesima.

Il sistema di individuazione degli incaricati prevede le seguenti azioni:

- Consegna delle indicazioni operative e delle istruzioni per lo svolgimento delle operazioni e per l'accesso ai sistemi informativi e ai dati scolastici, secondo il profilo professionale di inquadramento e l'area operativa alla quale si è assegnati ovvero viene chiesto di collaborare.
- Assegnazione di credenziali di autenticazione con conseguente abilitazione all'accesso a sistemi informativi e applicativi scolastici.
- Formazione specifica sulla corretta modalità di trattamento dei dati personali.

Ciascun incaricato del trattamento individuato all'interno dell'IC RINNOVATA PIZZIGONI è stato formalmente nominato da parte del Titolare del trattamento. Le norme generali di comportamento sono sottoscritte a tutti gli incaricati al momento della nomina.

Si riporta la sintesi dei compiti e delle responsabilità per la tutela dei dati.

Responsabilità	Soggetto Individuato
Preparazione e invio lettere per gli incaricati	Titolare del trattamento supporto Referente Privacy
Preparazione e invio lettere a Responsabili Esterni	Titolare del trattamento supporto Referente Privacy
Aggiornamento della documentazione Privacy	Titolare del trattamento supporto Referente Privacy
Supervisione e controllo periodico della corretta gestione dei dati da parte degli incaricati	Titolare del trattamento supporto Referente Privacy
Supervisione e coordinamento delle attività di informazione/formazione	Titolare del trattamento supporto Referente Privacy
Registrazione dei backup	Amministratore di Sistema
Archiviazione dei backup	Amministratore di Sistema
Creazione ID e gestione password e accessi	Amministratore di Sistema
Ripristino dati da backup	Amministratore di Sistema
Gestione di virus e antivirus	Amministratore di Sistema

9 SICUREZZA DEI DATI PERSONALI

9.1 Sicurezza del trattamento

Il Titolare del trattamento e il Responsabile del trattamento, in conformità all'articolo 32 del Regolamento UE 679/2016, hanno messo in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio. Le misure adottate garantiscono inoltre:

a) La pseudonimizzazione e la cifratura dei dati personali, ove possibile.

b) La capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento.

c) La capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico.

d) Una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Il Titolare del trattamento e il Responsabile del trattamento assicurano che chiunque agisce sotto lo loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal Titolare del trattamento.

La sicurezza "*è l'insieme delle misure atte a garantire la disponibilità, l'integrità e la riservatezza delle informazioni gestite*".

Sono tre gli aspetti fondamentali relativi alla sicurezza delle informazioni:

- **Riservatezza**: solo gli utenti autorizzati possono accedere alle informazioni necessarie.
- **Integrità**: tutela dell'accuratezza e completezza dei dati.
- **Disponibilità**: le informazioni sono rese disponibili quando occorre e nell'ambito di un contesto pertinente.

Si riportano di seguito le misure di sicurezza adottate nell'ambito del trattamento dei dati effettuato dall'IC RINNOVATA PIZZIGONI.

9.1.1 Gestione operativa - misure di sicurezza fisica

Misure di sicurezza fisica	Note
Accesso agli uffici ove sono effettuati i trattamenti	Presente – chiusura a chiave
Sistemi di allarme/antintrusione	Presenti – allarme su plesso Rinnovata
Reception	Presente
Registrazione degli accessi all'Ufficio	Presente
Autenticazione degli accessi all'Ufficio	Presente
Chiusura delle porte locale server	Presente – chiusura a chiave; il server è contenuto in segreteria all'interno di un armadio *rack*
Protezioni antisfondamento vetri	Non presente
Custodia in classificatori o armadi chiusi a chiave	Presente
Custodia dati in armadi blindati/ignifughi	Non presente
Dispositivi antincendio	Presente
Porte tagliafuoco	Presente
Gruppo di continuità	Presente
Schermatura cavi	Presente
Messa a terra	Presente
Climatizzazione sala server	Presente
Presidio personale esterno	Non presente

Sala server situata in luogo non soggetto ad allagamenti	Vedi sopra
Distruggi documenti	Presente

9.1.2 Gestione operativa - misure di sicurezza logica

Misure di sicurezza logica	Note
Identificazione dell'Incaricato e/o Utente	Presente - utenze nominali
Autentificazione dell'Incaricato e/o Utente	Presente - utenze nominali
Profilazione utente	Non presente
Controllo degli accessi a dati e programmi	Presente
Registrazione degli accessi	Presente
Controlli aggiornati antivirus	Presente – aggiornamento presente con cadenza giornaliera
Sottoscrizione elettronica	Presente
Cifratura dei dati memorizzati	Presente
Cifratura dei dati trasmessi	Presente
Annotazione della fonte dei dati	Presente
Annotazione del Responsabile dell'operazione	Presente
Monitoraggio continuo delle sessioni di lavoro	Non presente
Sospensione automatica delle sessioni di lavoro e riavvio con password	Presente - sospensione dopo 10 minuti di inattività e richiesta di password al riavvio
Verifiche periodiche sulle autorizzazioni dati e/o trattamenti consentiti	Presenti in occasione di consulenza in materia privacy svolti dal DPO
Firewall	Presente
Inibizione accessi simultanei con medesimo account	Non presente
Sospensione automatica degli account	Non presente
Manutenzione sistemi e software	Presente
Sistemi di rilevazione disfunzioni	Firewall / antivirus /antimalware
Sistemi di rilevazione intrusione	Firewall / antivirus /antimalware

9.1.3 Gestione operativa - misure di sicurezza organizzativa

Il datore di lavoro ha adottato misure organizzative e fisiche idonee a garantire che:

Misure di sicurezza organizzativa	Note
Analisi dei rischi	Nel presente documento
Classificazione dei dati	Nel presente documento
Linee guida per la sicurezza delle informazioni	Regolamento interno
Linea guida su utilizzo degli strumenti scolastici	Regolamento interno
Linee guida posta elettronica e internet	Regolamento interno
Assegnazione di incarichi	Lettere di nomina
Mansionari e/o altre istruzioni interne	Descrizione della mansione tramite il contratto
Formazione	Non presente
Backup e disaster recovery	Procedura
Piano di manutenzione impianti	Presente
Dichiarazione conformità impianti	Presente
Procedure accessi	Presente
Distruzione dei rifiuti elettrici ed elettronici in caso di smaltimento	In caso di smaltimento di rifiuti elettrici ed elettronici, l'effettiva cancellazione dei dati personali dai supporti contenuti nelle

	apparecchiature elettriche ed elettroniche avviene. In particolare è previsto che, se ancora funzionante, il disco fisso viene asportato e riformattato per futuri utilizzi. Lo smaltimento di altri supporti di memorizzazione di tipo ottico o magneto-ottico avviene tramite distruzione fisica
Assegnazione chiavi e codici	Regolamento interno
Politiche e procedure di sviluppo software	Non presente
Audit interni	Presenti in occasione di consulenza in materia privacy svolti dal DPO
Controllo trattamenti effettuati da soggetti terzi	Lettere di nomina ai responsabili esterni del trattamento (elencate nel presente documento)

9.1.4 Gestione operativa - misure fisiche ed organizzative per il trattamento dei dati cartacei

Tutti gli armadi e i classificatori contenenti dati personali riservati sono ad accesso selezionato e muniti di serratura con chiavi custodite da personale individuato. Gli armadi e i classificatori della sede che risultassero non chiusi sono ubicati in uffici ad accesso selezionato. Si riporta la tabella delle responsabilità per la gestione degli archivi:

Archivio / armadio	**Collocazione**	**Responsabile**
Personale docente e ATA	Ufficio Segreteria	Personale Direzione
Alunni e famiglie	Uffici Segreteria e Didattica	Personale Direzione
Messe a disposizione	Ufficio Segreteria	Personale Direzione
Fornitori e collaboratori	Ufficio Segreteria	Personale Direzione

Il Regolamento d'Istituto per la sicurezza delle informazioni viene distribuito a tutti gli incaricati al fine di garantire che:

- i luoghi ove si svolge il trattamento di dati personali dei lavoratori sono opportunamente protetti da indebite intrusioni;
- le comunicazioni personali riferibili esclusivamente a singoli lavoratori avvengano con modalità tali da escluderne l'indebita presa di conoscenza da parte di terzi o di soggetti non designati quali incaricati;
- siano impartite chiare istruzioni agli incaricati in ordine alla scrupolosa osservanza del segreto d'ufficio, anche con riguardo a dipendenti del medesimo datore di lavoro che non abbiano titolo per venire a conoscenza di particolari informazioni personali;
- sia prevenuta l'acquisizione e riproduzione di dati personali trattati elettronicamente, in assenza di adeguati sistemi di autenticazione o autorizzazione e/o di documenti contenenti informazioni personali da parte di soggetti non autorizzati;
- sia prevenuta l'involontaria acquisizione di informazioni personali da parte di terzi o di altri dipendenti.

9.1.5 Dati sanitari dei dipendenti

I dati particolari dei dipendenti trattati nell'ambito del rapporto di lavoro, sono conservati separatamente da ogni altro dato personale dell'interessato, accessibile solo da parte del personale autorizzato. Ciò trova attuazione anche con riferimento ai fascicoli personali cartacei dei dipendenti (ad esempio, utilizzando sezioni appositamente dedicate alla custodia dei dati particolari, inclusi quelli idonei a rivelare lo stato di salute del lavoratore) da conservare separatamente o in modo da non consentirne una indistinta consultazione nel corso delle ordinarie attività amministrative. Le cartelle sanitarie di rischio sono conservate presso la Direzione ad accesso esclusivo del Medico Competente.

10 VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI (P.I.A)

10.1 Fondamento giuridico

Il Regolamento 679/2016, all'articolo 35, richiede al Titolare del trattamento, allorché preveda di utilizzare nuove tecnologie per il trattamento dei dati personali, di effettuare, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali.

In particolar modo, la valutazione di impatto sulla protezione dei dati è richiesta nei seguenti casi:

- Una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche.
- Il trattamento su larga scala di categorie particolari di dati personali di cui all'articolo 9, o di dati relativi a condanne penali e a reati di cui all'articolo 10.
- La sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Poiché alcuni dei trattamenti eseguiti dal Titolare, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, potrebbero comportare rischi elevati per i diritti e le libertà delle persone fisiche, si è ritenuto di procedere ad effettuare un Privacy Impact Assessment. Tale documento, appena redatto, sarà allegato al presente documento.

Si ritiene opportuno anticipare un'analisi generica dei rischi all'interno di questo documento (cap. 11).

11 ANALISI DEI RISCHI

Al fine di mettere in atto le misure necessarie a garantire la sicurezza dei dati come patrimonio scolastico e a tutelare i diritti e le libertà degli interessati, anche per rischi non legati specificatamente al trattamento dei dati personali, si è proceduto a individuare le categorie di rischi connessi alla gestione dei dati, valutando potenziali impatti in termini di Riservatezza (R), Disponibilità (D), Integrità (I).

Tipologia evento	Descrizione fonte di rischio	Impatto		
		R	D	I
Eventi Fisici	Incendio		X	X
	Allagamento		X	
	Manomissione		X	
	Terremoti		X	
	Fulmini e scariche atmosferiche		X	
Malfunzionamenti servizi	Guasto impianto di condizionamento		X	
	Sbalzi di tensione		X	
	Eccesso di traffico sulla rete		X	
	Disturbi elettromagnetici		X	X
Furto di informazioni e strumentazione	Intercettazioni (anche attraverso stampante)	X		
	Furto hardware	X	X	
	Furto dispositivi mobili	X	X	
	Furto di memorie o supporti esterni	X		
Anomalie IT	Malfunzionamento strumentazione IT		X	X
	Saturazione dei sistemi		X	X
	Malfunzionamenti applicativi scolastici	X	X	X
	Errori di manutenzione	X	X	X
	Virus e malware su pc	X	X	X
	Virus e malware su dispositivi mobili	X	X	X
	Non adeguata formattazione hw dismesso	X		
	Scadenza licenza software, interruzione degli aggiornamenti sulla sicurezza	X		X
Organizzazione /comportamento	Indisponibilità del personale		X	
	Cambio di personale	X	X	
	Rivelazione di informazioni a persone non autorizzate	X		
	Ricezione dati da origini non affidabili	X		
	Cancellazione erronea dei file		X	X
	Salvataggio file per uso personale	X		
Azioni non autorizzate	Uso non autorizzato dispositivi scolastici	X	X	X
	Uso di software non autorizzati	X	X	X
	Alterazione volontaria di informazioni	X	X	X
	Accesso non autorizzato alla rete	X		X
	Uso di strumentazione da parte di non autorizzate	X		X
	Accesso al DB da parte di non autorizzati	X		X
	Informazioni raccolte a seguito di non adeguata protezione all'insaputa dell'utente (es. senza screen saver)	X		
Uso non autorizzato di documenti cartacei	Fotocopie non autorizzate	X		
	Recupero di documenti scartati	X		
	Sottrazione di documenti cartacei	X		
	Riutilizzo di stampe contenenti dati personali	X		

Si riportano i criteri per definire il livello di impatto connesso agli eventi sopra descritti.
La probabilità di accadimento "P" è stabilita dall'analisi della storia recente dell'organizzazione, dalle segnalazioni dalle autorità di controllo e dalle linee guida e dai riferimenti bibliografici richiamati.

Livello	P – Probabilità di accadimento (almeno uno dei seguenti scenari)
1 Basso	- l'evento si può verificare con frequenza inferiore rispetto a quanto riportato dalle ricerche più note; - in caso di attacco deliberato, i dati sono poco appetibili e l'immagine aziendale non è compromessa e pertanto i tentativi di attacco o non sono iniziati o sono condotti da malintenzionati scarsamente preparati da un punto di vista tecnico e con scarse risorse a disposizione; - in caso di attacco non deliberato, l'ambito è poco complesso e quindi è difficile commettere errori; - in caso di eventi naturali, gli studi dimostrano che la minaccia può verificarsi molto raramente.
2 Medio	- la minaccia si può verificare secondo quanto riportato dalle ricerche più note; - in caso di attacco deliberato, i dati sono poco appetibili e l'immagine aziendale non è compromessa e quindi può essere condotto da malintenzionati non particolarmente motivati, mediamente preparati da un punto di vista tecnico e con scarse risorse a disposizione; o in alternativa, gli studi confermano che tentativi di attacco sono comunque rari; - in caso di attacco non deliberato, l'ambito è mediamente complesso e quindi possono essere commessi errori; - in caso di eventi naturali, gli studi dimostrano che la minaccia può verificarsi nella media dei casi studiati.
3 Alto	- la minaccia si può verificare più frequentemente rispetto a quanto riportato dalle ricerche più note; - in caso di attacco deliberato, i dati sono appetibili o l'immagine aziendale è compromessa, e quindi può essere condotto da malintenzionati molto motivati, tecnicamente preparati e con ingenti risorse a disposizione; o in alternativa, gli studi confermano che tentativi di attacco sono comunque portati molto di frequente; - in caso di attacco non deliberato, l'ambito è di elevata complessità (per esempio per molteplicità di sedi, tipologie di sistemi informatici, utenti interni e/o esterni) e quindi è facile siano commessi errori; - in caso di eventi naturali, gli studi dimostrano che la minaccia si verifica quasi certamente.

Si riportano i criteri per definire il livello di impatto connesso agli eventi sopra descritti.

D – Entità del danno			
Livello	**R- Riservatezza**	**I - Integrità**	**D- Disponibilità**
1 Basso	**Organizzazione** I dati non presentano particolari requisiti di riservatezza. I dati sono pubblici. **Interessati** La mancanza di riservatezza ha impatti lievi (p.e. fastidio) sulla vita sociale o personale degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di libertà; - danni fisici; - stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.	**Organizzazione** I dati non presentano particolari requisiti di integrità. I dati gestiti non fanno parte di transazioni economiche, finanziarie o sanitarie. **Interessati** La mancanza di integrità ha impatti lievi (p.e. fastidio) sulla vita sociale o personale degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di libertà; - danni fisici; - stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.	**Organizzazione** L'indisponibilità dei dati oltre i tempi stabiliti contrattualmente non comporta multe o penali rilevanti. **Interessati** La mancanza di disponibilità ha impatti lievi (p.e. fastidio) sulla vita sociale o personale degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di libertà; - danni fisici; - stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.
2 Medio	**Organizzazione** I dati devono essere riservati per ragioni di business (concorrenza sleale, danni all'immagine), ma un'eventuale loro diffusione non ha elevati impatti sul business dell'organizzazione, sul rispetto della normativa vigente o sull'immagine dell'organizzazione. **Interessati** La mancanza di riservatezza ha impatti, non critici (p.e. perdita di tempo, perdita limitata di serenità), sulla vita sociale o personale degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di libertà; - danni fisici; - stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.	**Organizzazione** I dati non sono oggetto di transazioni di tipo economico, finanziario o sanitarie con impatti sul business di un'impresa. La mancanza di integrità dei dati non ha elevati impatti sulle attività operative o sul rispetto della normativa vigente. **Interessati** La mancanza di integrità ha impatti, non critici (p.e. perdita di tempo, perdita limitata di serenità), sulla vita sociale o personale degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di libertà; - danni fisici; - stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.	**Organizzazione** L'indisponibilità dei dati oltre i tempi stabiliti contrattualmente comporta multe o penali non particolarmente rilevanti. **Interessati** La mancanza di disponibilità ha impatti, non critici (p.e. perdita di tempo, perdita limitata di serenità), sulla vita sociale o personale degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di libertà; - danni fisici; - stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.

D – Entità del danno			
Livello	**R- Riservatezza**	**I - Integrità**	**D- Disponibilità**
3 Alto	**Organizzazione** I dati devono essere riservati per ragioni di business (concorrenza sleale, danni all'immagine) e un'eventuale loro diffusione ha elevati impatti sul business dell'organizzazione, sul rispetto della normativa vigente o sull'immagine dell'organizzazione **Interessati** La mancanza di riservatezza ha elevato impatto sulla vita sociale (p.e. sconvolgendola) o personale degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di libertà; - danni fisici; - stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.	**Organizzazione** I dati non sono oggetto di transazioni di tipo economico, finanziario o sanitarie con impatti sul business di un'impresa. La mancanza di integrità dei dati ha elevati impatti sulle attività operative o sul rispetto della normativa vigente. **Interessati** La mancanza di integrità ha elevato impatto sulla vita sociale (p.e. sconvolgendola) o personale degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di libertà; - danni fisici; - stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.	**Organizzazione** L'indisponibilità dei dati oltre i tempi stabiliti contrattualmente comporta multe o penali rilevanti. **Interessati** La mancanza di disponibilità ha elevato impatto sulla vita sociale (p.e. sconvolgendola) o personale degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di libertà; - danni fisici; - stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.
4 Critico	**Organizzazione** La diffusione delle informazioni ha elevati impatti sul business dell'organizzazione o sul rispetto della normativa vigente o sull'immagine dell'organizzazione tali da compromettere la sostenibilità dell'organizzazione. **Interessati** La mancanza di riservatezza ha impatto sulla sopravvivenza degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di libertà; - danni fisici; - stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.	**Organizzazione** La mancanza di integrità delle informazioni ha elevati impatti sul business aziendale o sul rispetto della normativa vigente tali da compromettere la sostenibilità dell'organizzazione. **Interessati** La mancanza di integrità ha impatto sulla sopravvivenza degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di libertà; - danni fisici; - stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.	**Organizzazione** L'indisponibilità dei dati oltre i tempi stabiliti contrattualmente comporta multe o penali che mettono in pericolo la sostenibilità economica e di immagine o hanno impatti sulla sicurezza delle persone fisiche. **Interessati** La mancanza di disponibilità ha impatto sulla sopravvivenza degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di libertà; - danni fisici; - stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.

Si riporta la stima della probabilità degli eventi sopra riportati, tenuto conto del potenziale impatto in termini di danno nei confronti dell'interessato e il conseguente livello di rischio associato.

Fattore di rischio	Probabilità	Impatto	Livello di rischio
Eventi fisici	2	3	6
Malfunzionamenti servizi	2	3	6
Furto di informazioni e strumentazione	2	3	6
Anomalie IT	2	3	6
Organizzazione /comportamento	2	3	6
Azioni non autorizzate	2	3	6
Uso non autorizzato di documenti cartacei	2	3	6

Valutazione dei livelli di rischio

P/D	Basso	Medio	Alto/Critico
Basso			
Medio			
Alto			

Livelli di rischio individuati e definizione dei controlli

1-2	Basso	Non necessitano interventi (buone prassi)
3-6	Medio	Azioni periodiche e programmate (Controllo operativo)
8-9	Alto	Azioni a breve termine
≥ 12	Critico	Azioni di immediata attuazione

12 DATA BREACH – Notifica della violazione dei dati all'autorità di controllo

Il Regolamento, all'art. 33 definisce che in caso di violazione dei dati personali, il Titolare o il Responsabile del trattamento procede senza indebiti ritardi e, ove possibile, non oltre 72 ore dopo esserne venuto a conoscenza, notifica la violazione dei dati personali all'autorità di controllo competente ai sensi dell'articolo 55, a meno che è improbabile che la violazione dei dati personali comporti un rischio per i diritti e le libertà delle persone fisiche. Se la notifica all'autorità di controllo non viene effettuata entro 72 ore, è accompagnata dai motivi del ritardo.

La notifica riporta i seguenti elementi:

a) descrizione della natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati e le categorie e il numero approssimativo di dati personali in questione;
b) nome e contatti del referente del Titolare o del Responsabile della Protezione dei Dati (DPO);
c) descrizione delle probabili conseguenze della violazione dei dati personali;
d) descrizione delle misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per
e) attenuarne i possibili effetti negativi.

Il DataBreach può riguardare essenzialmente:

- Riservatezza dei dati – divulgazione o accesso non autorizzato o accidentale di dati personali
- Disponibilità dei dati – alterazione non autorizzata o accidentale di dati personali
- Integrità dei dati – perdita accidentale o accesso non autorizzato di dati personali

La violazione può potenzialmente avere una serie di effetti negativi significativi sugli individui, che possono provocare danni fisici, materiali o immateriali, come ad esempio:

- perdita del controllo sui propri dati personali
- limitazione dei diritti
- discriminazione
- furto d'identità
- frode
- perdita finanziaria
- inversione non autorizzata di pseudonimizzazione
- danno alla reputazione
- perdita di riservatezza dei dati personali protetti dal segreto professionale.

Ogni possibile violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio sono riportate nel registro delle violazioni, compilato a cura del Titolare del trattamento.

13 TRASFERIMENTO DATI EXTRA UE

L'IC RINNOVATA PIZZIGONI non effettua alcun trasferimento di dati personali fuori dal territorio dell'Unione Europea.
In caso di trasferimento di dati personali a un Paese terzo saranno in ogni caso messe in atto adeguate misure di sicurezza. È possibile richiedere ulteriori informazioni a tale riguardo e ottenere una copia delle relative salvaguardie attraverso l'invio di una richiesta ai contatti forniti dal Titolare del trattamento.

14 GESTIONE DEI DIRITTI DELL'INTERESSATO

L'IC RINNOVATA PIZZIGONI, in qualità di Titolare del trattamento, ha fornito a tutti gli interessati tutte le informazioni di cui agli articoli 13 e 14 del Regolamento Europeo 2016/679 e le comunicazioni di cui agli articoli 15 a 22 tramite l'informativa.

L'interessato può esercitare i suoi diritti contattando direttamente il Titolare del trattamento all'indirizzo di posta elettronica: segreteria@scuolarinnovata.it

Al fine di garantire i diritti degli interessati, il Titolare del trattamento, supportato da eventuali Responsabili del trattamento o dal DPO, coinvolge le funzioni scolastiche che possono fornire le risposte alle richieste degli interessati.

14.1 Diritto di accesso

Il Titolare del trattamento ha adottato misure idonee al fine di garantire agli interessati il diritto di ottenere la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di esercitare il "diritto di accesso" così come riconosciuto dall'articolo 15 del Regolamento UE 679/2016. L'interessato ha pertanto diritto di ottenere l'accesso ai dati personali che lo riguardano e alle seguenti informazioni:

a) Le finalità del trattamento.
b) Le categorie di dati personali in questione.
c) I destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali.
d) Quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo.

e) L'esistenza del diritto dell'interessato di chiedere al Titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento.

f) Il diritto di proporre reclamo a un'autorità di controllo.

g) Qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine.

h) L'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4 e almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

14.2 Diritto di rettifica

L'interessato, così come disposto dall'articolo 16 del Regolamento Europeo 679/2016, ha il diritto di ottenere dal Titolare del trattamento la rettifica dei dati personali inesatti e, tenuto conto delle finalità del trattamento, ha altresì il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

14.3 Diritto all'oblio

L'interessato, così come disposto dall'articolo 17 del Regolamento 679/2016, ha il diritto di ottenere dal Titolare del trattamento la cancellazione dei dati personali che lo riguardano qualora sussistano uno dei seguenti motivi:

a) I dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati.

b) L'interessato revoca il consenso su cui si basa il trattamento e se non sussiste altro fondamento giuridico per il trattamento.

c) L'interessato si oppone al trattamento e non sussiste alcun motivo legittimo prevalente per procedere al trattamento.

d) I dati personali sono stati trattati illecitamente.

e) I dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il Titolare del trattamento.

f) I dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8.

14.4 Diritto di limitazione di trattamento

L'interessato, così come disposto dall'articolo 18 del Regolamento 679/2016, ha il diritto di ottenere dal Titolare del trattamento la limitazione del trattamento quando:

a) L'interessato contesta l'esattezza dei dati personali, per il periodo necessario al Titolare del trattamento per verificare l'esattezza di tali dati personali.

b) Il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo.

c) Benché il Titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

d) L'interessato si è opposto al trattamento ai sensi dell'articolo 21 in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del Titolare del trattamento rispetto a quelli dell'interessato.

14.5 Diritto alla portabilità dei dati

L'interessato, così come disposto dall'articolo 20 del Regolamento 679/2016, ha il diritto di ricevere i dati personali che lo riguardano forniti a un Titolare del trattamento e ha altresì il diritto di trasmettere tali dati a un altro Titolare del trattamento senza impedimenti da parte del Titolare del trattamento cui li ha forniti.

14.6 Diritto di opposizione

L'interessato, così come disposto dall'articolo 21 del Regolamento 679/2016, ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano.

L'interessato può esercitare il suo diritto contattando direttamente il Titolare del trattamento (ISTITUTO COMPRENSIVO RINNOVATA PIZZIGONI).

15 FORMAZIONE

15.1 Contesto generale

Tale capitolo del documento viene redatto al fine di definire le modalità di identificazione delle esigenze ed i criteri di attuazione del processo di addestramento del personale per il perseguimento delle strategie nel pieno rispetto della normativa vigente sul trattamento dei dati.

Scopo di questa attività è, inoltre, informare e formare costantemente il personale sui compiti assegnati, sulle responsabilità e sulle metodologie da applicare nell'esecuzione delle proprie attività, nell'ottica di un miglioramento continuo delle attività lavorative.

15.2 Gestione Operativa

Il personale verrà coinvolto in un processo di formazione/informazione in modo da assicurare la professionalità e le adeguate capacità degli incaricati per svolgere le attività di propria competenza.

In questo senso, l'attività formativa è rivolta a:

a) Fornire una preparazione professionale di base necessaria allo svolgimento dei compiti assegnati.
b) Permettere un continuo aggiornamento tecnico, reso necessario dall'evoluzione delle conoscenze tecniche ed informatiche.
c) Assicurare la corretta comprensione ed applicazione dei principi su cui si basa la Policy scolastica stabilita per il trattamento dei dati.

L'addestramento è previsto per:

d) Personale di nuova assunzione (comprensivo dell'affiancamento a persona esperta).
e) Personale assegnato a nuove mansioni.
f) Introduzione di nuove tecnologie informatiche.

Il regolamento sull'uso dei sistemi informatici è consegnato ad ogni collaboratore, all'atto dell'avvio del rapporto di lavoro, insieme al regolamento interno.
Considerare procedure specifiche sulla dimissione del collaboratore, gestione lunga assenza e cambio mansione.

16 MONITORAGGIO PERIODICO

Periodicamente, con l'eventuale supporto dell'Amministratore di Sistema o altre funzioni scolastiche, il Titolare del trattamento o DPO effettua delle verifiche sul corretto stato di applicazione delle procedure previste per il trattamento dei dati, verificando ad esempio le configurazioni di pc e dati trattati. Le verifiche sulla corretta applicazione dei principi relativi al trattamento dei dati si effettuano inoltre in occasione dell'aggiornamento annuale del presente documento.

A seguito di tali verifiche il Titolare del trattamento, in collaborazione con le funzioni coinvolte, stabilisce dei piani di miglioramento atti a prevenire il verificarsi di eventuali non conformità e a fornire una formazione continua al personale coinvolto nel trattamento dei dati.

17 PROGRAMMA DI MIGLIORAMENTO

In riferimento a quanto esposto nel capitolo 11 del presente documento, nella tabella sottostante viene riportato il programma individuato none società per il continuo miglioramento del sistema implementato:

Fattore di rischio	Probabilità	Impatto	Livello di rischio
Eventi fisici	2	3	6
Malfunzionamenti servizi	2	3	6
Furto di informazioni e strumentazione	2	3	6
Anomalie IT	2	3	6
Organizzazione /comportamento	2	3	6
Azioni non autorizzate	2	3	6
Uso non autorizzato di documenti cartacei	2	3	6

Fattore di Rischio	Descrizione intervento	Termine attuazione	Responsabile attuazione
Eventi fisici	Si consiglia di monitorare periodicamente gli adempimenti in materia di sicurezza sui luoghi di lavoro	Gennaio 2021	Titolare del trattamento con supporto RSPP
Malfunzionamento di servizi	Si consiglia di monitorare periodicamente il corretto funzionamento delle apparecchiature scolastiche		Titolare del trattamento con supporto del personale addetto
Furto di informazioni e strumentazione	Si consiglia di monitorare periodicamente l'accesso alla sede e i dispositivi scolastici		
Anomalie IT	Si consiglia di monitorare periodicamente la sicurezza dei sistemi informatici scolastici		Titolare del trattamento con supporto Amministratore di Sistema
Organizzazione comportamento	Si consiglia di monitorare periodicamente il corretto utilizzo dei dispositivi e degli archivi scolastici da parte del personale		Titolare del trattamento con supporto del personale addetto
Azioni non autorizzate			
Uso non autorizzato di documenti cartacei			
Organizzazione /comportamento	Aggiornamento del Regolamento aziendale per la gestione dei dati	Maggio 2021	Titolare del Trattamento

18 ALLEGATI AL MODELLO ORGANIZZATIVO

Si riportano gli allegati al modello organizzativo per la gestione privacy dell'IC RINNOVATA PIZZIGONI

LT	Informativa e consenso personale docente e ATA
LT	Informativa MAD
LT	Informativa alunni e famiglie
LT	Informativa collaboratori P.I.
LT	Informativa bandi
LT	Nomina persone autorizzate al trattamento (docenti-Ata-collab.scolastici)
LT	Nomina Responsabile esterno del trattamento
LT	Nomina Amministratore di Sistema
LT	Privacy e Cookies Policy per il sito internet
LT	Contatti DPO
LT	Informativa COVID19 (inserita nel protocollo COVID)
PO	Regolamento per l'utilizzo dei sistemi informativi
RG	Registro delle attività di trattamento
RG	Registro delle violazioni
PO	Procedura per l'esercizio dei diritti da parte dell'interessato
PO	Procedura per la gestione Data Breach

19 NOTA FINALE

Data Luogo

_____ _____

Titolare del trattamento dei dati

_____