Ministero dell'Istruzione e del Merito
Ufficio Scolastico Regionale per il Lazio
ISTITUTO COMPRENSIVO "NELSON MANDELA"
Infanzia, - Primaria - Secondaria di 1° grado
Via dei Torriani, 44 – 00164 Roma Tel. 0666000349
Cod. Mecc. RMIC8FW00E – C.F. 97712890587
rmic8fw00e@istruzione.it - rmic8fw00e@pec.istruzione.it
www.icnelsonmandela.edu.it

DISCIPLINARE sulla sicurezza dei dati personali

[secondo le disposizioni del CODICE IN MATERIA DI DATI PERSONALI (D.Leg.vo 196/2003), della Legge 35/2012 e del DISCIPLINARE TECNICO (ALL B)] così come rivisto ex REGOLAMENTO EUROPEO 2016 679

Giuseppe Renato CROCE DATA PROTECTION OFFICIER
2022-2023-2024

PARTE GENERALE

SOMMARIO

PREMESSE

Questo Documento detta le disposizioni idonee alla adozione delle misure di sicurezza organizzative, fisiche e logiche necessarie a tutelare e prevenire i rischi nel trattamento dei dati personali e sensibili effettuato dall'Istituto Scolastico, ed in relazione, altresì, alla finalità di proteggere gli archivi elettronici contenenti i dati personali degli interessati, così come stabilito dagli artt. 33-36 del D.Lgs n.196 del 30 giugno 2003 s.m.i. e rivisti dalla Legge 35/2012. Nella procedura si è tenuto conto delle seguenti misure previste dall'art 34 del D.Lgs n.196/2003 s.m.i. così come rivisto dalla Legge 35/2012 e alla luce altresì dei principi dettati dal REGOLAMENTO EUROPEO 2016 679:

a) autenticazione informatica;

b) adozione di procedure di gestione delle credenziali di autenticazione;

c) utilizzazione di un sistema di autorizzazione;

d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;

e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;

f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;

g) tenuta di un aggiornato documento programmatico sulla sicurezza;

h) adozione di tecniche di cifratura o di codici identificativi per

determinati trattamenti di dati idonei a rivelare lo stato di salute effettuati da organismi sanitari o la vita sessuale.

Il sistema informatico descritto nel presente documento deve, quindi, ritenersi sicuro, in quanto garantisce la disponibilità, l'integrità e l'autenticità, nonché la riservatezza dell'informazione e dei servizi per il trattamento, soprattutto in

riferimento all'attribuzione di specifici incarichi, alla certificazione delle fonti di provenienza dei dati e le istruzioni per le persone autorizzate ad effettuare i trattamenti. Il monitoraggio del sistema informatico assicura inoltre la tempestiva eliminazione delle anomalie che dovessero eventualmente manifestarsi.

GLOSSARIO

- **Banca di dati**

qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti (gli archivi cartacei o elettronici/informatici) che contengono i dati oggetto di trattamento);

- **Interessato**

la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;

- **Dati personali**

qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;

- **Dati identificativi**

i dati personali che permettono l'identificazione diretta dell'interessato;

- **Dato anonimo**

il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabili;

- **Dati sensibili**

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;

- **Dati giudiziari**

i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;

- **Diffusione**

il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma;

- **Garante per la protezione dei dati personali**

Autorità posta a garanzia del rispetto delle norme sulla privacy. E' un organo collegiale costituito da quattro membri (commissari) e da un Segretario Generale. Il Garante opera in piena autonomia e con indipendenza
di giudizio e di valutazione. Riceve, tra l'altro, le segnalazioni ed i ricorsi da parte degli interessati in relazione a presunte violazioni della normativa (dinieghi di "accesso" e/o trattamenti illeciti), emettendo al riguardo eventuali provvedimenti nei confronti del Titolare/Responsabile.

- **Titolare del trattamento**

la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;

- **Responsabile della sicurezza dei dati informatici**

la persona incaricata della definizione e della realizzazione della politica di sicurezza. Coincide colla figura del Titolare del trattamento che normalmente, a sua volta, designa l'**Amministratore del sistema informatico;**

- **Responsabile del trattamento**

il soggetto preposto dal titolare del trattamento dei dati personali. La designazione di un responsabile è facoltativa e non esonera da responsabilità il titolare, il quale ha comunque l'obbligo di impartirgli precise istruzioni e di

vigilare sull'attuazione di queste. Il responsabile deve essere un soggetto che fornisce, per esperienza, capacità e affidabilità, idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. Il responsabile del trattamento dei dati personali, ai fini della sicurezza, ha le responsabilità indicate nella lettera di incarico;

- **Amministratore del sistema informatico**

il soggetto cui è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di base dati e di consentirne l'utilizzazione. In questo contesto l'amministratore di sistema assume anche le funzioni di amministratore di rete, ovvero del soggetto che deve sovrintendere alle risorse di rete e di consentirne l'utilizzazione. L'amministratore deve essere un soggetto fornito di esperienza, capacità e affidabilità nella gestione delle reti

- **Custode delle password**

il soggetto cui è conferito la gestione delle password degli incaricati del trattamento dei dati in conformità ai compiti indicati nella lettera di incarico;

- **Incaricato delle copie di sicurezza delle banche dati**

il soggetto che ha il compito di sovrintendere alla esecuzione periodica delle copie di sicurezza delle banche di dati;

- **Incaricati del trattamento dei dati personali**

le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare del trattamento o dal responsabile del trattamento;

- **Sicurezza dei dati personali**

il legislatore ha introdotto una prima norma generale sulla sicurezza dei dati nell'ambito dell'articolo 31 del Codice della privacy, affermando subito: " *per essere efficace, la protezione dei dati deve comprendere anche una disciplina rigorosa della sicurezza* ". Ha dettato poi i singoli adempimenti nei successivi articoli 32-36 e nell'allegato B del Codice.

In particolare, il suddetto allegato B, intitolato "***Disciplinare tecnico in materia di misure minime di sicurezza***", disciplina in maniera puntuale e rigorosa le misure minime da adottare per garantire la sicurezza fisica, logica e organizzativa dei dati

personali. L'intera disciplina è ispirata al principio generale sancito dal citato articolo 31, secondo il quale: *"i dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle*
specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso
non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta".
Le modalità operative e le informazioni di carattere tecnico in materia di misure minime di sicurezza vengono rese disponibili nelle istruzioni agli **Incaricati del trattamento dei dati personali comuni, sensibili e/o giudiziari.**

Sanzioni

Le sanzioni previste dalla normativa vigente (di cui agli articoli da 161 a 172 del Codice privacy) per gli inadempimenti o di trattamenti illeciti di dati personali possono essere, a seconda del tipo di inosservanza, di natura amministrativa (fino ad un massimo di 60.000 Euro) o penale (fino a 3 anni di reclusione).

2. LE FIGURE RESPONSABILI PER LA SICUREZZA DEI DATI PERSONALI

a. Titolare del Trattamento

Il Titolare del trattamento è il soggetto che, nel raccogliere i dati personali decide come ed in base a quali finalità effettuerà il trattamento dei dati raccolti. Pertanto ricopre il ruolo di **Responsabile della sicurezza dei dati** con le seguenti responsabilità e funzioni:

- Delineare finalità, modalità, strumenti utilizzati nel trattamento dati;
- Predisporre le misure di sicurezza da attuare per la protezione dei dati personali comprese le misure minime di sicurezza previste dall'allegato B del D.Lgs n.196/2003 s.m.i.;
- Redigere ed aggiornare periodicamente il documento programmatico sulla sicurezza con la specificazione delle sedi e degli uffici in cui viene effettuato il trattamento dei dati, l'elenco delle banche dati oggetto di trattamento, la descrizione del sistema informatico attraverso il quale avviene il trattamento dei dati personali;
- Vigilare sulla puntuale osservanza delle disposizioni e delle proprie istruzioni anche attraverso verifiche periodiche;
- Definire e verificare periodicamente le modalità di accesso ai locali in cui sono conservati e trattati dati personali e le misure di protezione da adottare;
- Decidere se affidare il trattamento dei dati all'esterno della struttura del titolare.

Il Titolare, nella sua funzione di Responsabile della sicurezza dei dati personali, può incaricare un **Amministratore del sistema informatico** che sovrintende alle risorse informatiche utilizzate per il trattamento dei dati.

b. L' Amministratore del sistema informatico

Il Titolare del trattamento, nella sua funzione di Responsabile della sicurezza dei dati personali, può nominare per iscritto uno o più **Amministratori del sistema informatico,** anche affidando l'incarico a soggetti esterni con il compito di :

- Definire quali modalità, strumenti politiche adottare per la protezione del sistema informatico e verificarne l'efficacia con cadenza almeno semestrale;

- Effettuare l'aggiornamento dei programmi degli elaboratori onde prevenire la vulnerabilità degli strumenti elettronici e correggerne i difetti con cadenza almeno semestrale;
- Proteggere gli elaboratori dal rischio di intrusione esterna da parte di persone non autorizzate mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale;
- Attivare, dietro disposizione del Responsabile del trattamento, le credenziali di autenticazione agli incaricati del trattamento;
- Revocare, dietro disposizione del Responsabile del trattamento, tutte le credenziali non utilizzate in caso di perdita della qualità che consentiva all'incaricato l'accesso ai dati personali;
- Revocare, dietro disposizione del Responsabile del trattamento, tutte le credenziali per l'accesso ai dati degli incaricati al trattamento nel caso di mancato utilizzo per oltre sei mesi;
- Informare il Responsabile della sicurezza dei dati personali nella eventualità che si siano rilevati dei rischi relativamente alle misure di sicurezza riguardanti i dati personali.

Al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita, l'Amministratore del sistema informatico deve definire la modalità e la periodicità di esecuzione delle copie di sicurezza oltre che le procedure di verifica delle copie fatte e di ripristino delle banche dati.

Qualora il Titolare/Responsabile della sicurezza ritenga di non nominare alcun Amministratore del sistema informatico, ne assumerà tutte le responsabilità e funzioni. La nomina dell'Amministratore del sistema informatico può essere a tempo determinato qualora esistano dei motivi che suggeriscano questa soluzione come nel caso di affidamento dell'incarico a soggetti esterni mediante sottoscrizione di contratto annuale.

c. Responsabile del trattamento

Il Titolare, nella sua funzione di Responsabile della sicurezza dei dati personali, ha facoltà di nominare uno o più **Responsabili del trattamento**; è altresì previsto che possa essere nominato "Responsabile" non solo una persona fisica ma anche una

società o altri organismi come gli enti, le associazioni, ecc.. Inoltre, la designazione può riguardare più soggetti (per esempio in presenza di una struttura molto articolata).
Il Titolare individua il Responsabile tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. Il responsabile effettua il trattamento attenendosi alle istruzioni ricevute dal Titolare del trattamento, impartendo istruzioni adeguate alle figure da esso nominate e vigilando sulla puntuale osservanza delle disposizioni e delle istruzioni impartite.
Il Responsabile del trattamento, in riferimento all'incarico ricevuto, assume le conseguenti responsabilità di:

- nominare per iscritto gli incaricati del trattamento per le banche dati che gli sono state affidate;
- nominare per iscritto uno o più incaricati delle copie di sicurezza delle banche dati;
- trasmettere ai propri incaricati le disposizioni ricevute dal Titolare in merito al trattamento di dati personali;
- sorvegliare che il trattamento sia effettuato nei termini e nei modi stabiliti dal Codice in materia di dati personali;
- Verificare periodicamente la sussistenza dei requisiti per la conservazione dei profili di autorizzazione degli Incaricati del trattamento

Il Responsabile del trattamento assume inoltre l'incarico di **custode delle copie delle credenziali** con il compito della:

- gestione e custodia delle credenziali per l'accesso ai dati degli Incaricati del trattamento;
- predisposizione, per ogni incaricato del trattamento, di una busta sulla quale è indicato il nome dell'incaricato e all'interno della busta deve essere indicata la credenziale usata. Le buste con le credenziali debbono essere conservate in luogo chiuso e protetto;
- istruzione degli incaricati del trattamento sull'uso delle parole chiave e sulle caratteristiche che debbono avere.

d. L' Incaricato delle copie di sicurezza delle banche dati

Il Responsabile del trattamento può nominare, se lo ritiene opportuno, uno o più **Incaricati delle copie di sicurezza delle banche dati** che hanno il compito di sovrintendere alla esecuzione periodica delle copie di sicurezza delle banche di dati.

Gli Incaricati delle copie di sicurezza delle banche dati devono:

- sovrintendere alla esecuzione periodica delle copie di sicurezza delle banche dati ad essi assegnate secondo le procedure definite dal responsabile della gestione del sistema informatico o, in assenza di tale figura, dal responsabile della sicurezza;
- Assicurarsi della qualità delle copie di sicurezza effettuate;
- attenersi alle disposizioni ricevute dal Responsabile del trattamento in merito alla conservazione delle copie delle banche dati;
- Provvedere a conservare e custodire con la massima cura i dispositivi utilizzati per le copie di sicurezza, impedendo l'accesso agli stessi dispositivi da parte di personale non autorizzato.
- Segnalare tempestivamente al Responsabile della gestione del sistema informatico ogni eventuale problema dovesse verificarsi nella normale attività di copia delle banche dati.

Qualora **il** Responsabile del trattamento ritenga di non nominare alcun Incaricato delle copie di sicurezza delle banche dati, ne assumerà tutte le funzioni e responsabilità.

e. L' Incaricato del trattamento dei dati personali

- Il Titolare od il Responsabile del trattamento possono nominare uno o più **Incaricati del trattamento dei dati personali**, persone fisiche autorizzate a compiere operazioni di trattamento sui dati personali con il compito di:
- Trattare i dati personali in modo lecito e secondo correttezza;
- Raccogliere e registrare i dati personali per scopi determinati, espliciti e legittimi, ed utilizzarli in altre operazioni del trattamento in termini compatibili con tali scopi;

- Verificare che siano esatti e, se necessario, aggiornarli;
- Verificare che siano pertinente completi e non eccedenti rispetto alle finalità per le quali sono raccolti e successivamente trattati;
- Conservarli in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti e successivamente trattati;

Nel caso in cui siano in possesso di autorizzazione all'utilizzo degli strumenti informatici, devono:

- Conservare con la massima segretezza le credenziali di autenticazione loro assegnate;
- Definire le parole chiave secondo i criteri fissati dal responsabile della sicurezza in collaborazione con l'Amministratore del sistema informatico. Le parole chiave vanno modificate al primo utilizzo e, successivamente almeno ogni 6 mesi (almeno ogni 3 mesi per i dati sensibili);
- custodire gli strumenti elettronici a loro affidati e non devono in nessun caso allontanarsi durante una sessione di trattamento di dati personali lasciando accessibile lo strumento elettronico;
- controllare e custodire gli atti e i documenti contenenti dati personali in modo da assicurarne l'integrità e la riservatezza.

Il Titolare o il Responsabile del trattamento devono consegnare a ciascun Incaricato del trattamento dei dati personali una copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina.

PARTE SPECIALE PRIMA

STRUTTURA ORGANIZZATIVA FUNZIONALE AL TRATTAMENTO DATI

SOMMARIO

1. Le Banche Dati dell'Istituto Scolastico

Tutti i dati posseduti vengono trattati esclusivamente presso gli Uffici dell'Istituto e nessuna altra struttura concorre al trattamento dei dati raccolti dall'Istituto. I dati possono essere comunicati a terzi solo nell'ambito della attività istituzionale dell'Istituto e comunque nei casi previsti dalla informativa fornita agli interessati od in seguito ad esplicito consenso espresso dagli stessi.

Le Banche contengono i seguenti Dati:

- ***Alunni:***

a. Documenti riguardanti gli alunni, relativi al corso di studi, alla presenza di handicap, alla certificazione dell'idoneità alla pratica sportiva non agonistica, alla scelta dell'insegnamento della religione cattolica, all'esito di scrutini, esami, piani educativi individualizzati differenziati
b. Documenti prodotti dalle famiglie riguardanti la certificazione della situazione patrimoniale e delle condizioni economiche.
c. Altri Rapporti scuola – famiglie
d. Organismi collegiali e commissioni istituzionali

- ***Dipendenti:***

a. Documentazione riguardante il personale docente e non docente, 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.
b. Gestione del contenzioso e procedimenti disciplinari

- ***Protocollo***
- ***Inventario***
- ***Magazzino***
- ***Rapporti con enti ed imprese***
- ***Fornitori*** :
- ***Dati per gestire le negoziazioni e le relative modalità di pagamento per la fornitura di beni e servizi***

- ***Contabilità e Bilancio***

Nel trattamento dei dati viene osservato quanto previsto nell'allegato "*Regolamento recante identificazione dei dati sensibili e giudiziari trattati e delle relative operazioni effettuate dall'Istituto Scolastico*"

2. Criteri di designazione dei soggetti sensibili

A. **Il Titolare del trattamento** ha ritenuto di nominare **l'Amministratore del sistema informatico** anche **Responsabile della Sicurezza del prefato Sistema.**
B. **Il Titolare del trattamento** ha ritenuto di nominare il Direttore dei Servizi Generali e Amministrativi **Responsabile del Trattamento** di tutte le Banche Dati sopra, prendendo atto, altresì, della necessità prospettata dal DSGA nelle funzioni di **Responsabile del Trattamento** di procedere alla nomina quali **Incaricati del trattamento dei dati** degli **"Assistenti Amministrativi"** nonché dei **"Collaboratori Scolastici"**. Questi ultimi in riferimento al trattamento di dati personali in occasione della gestione delle comunicazioni telefoniche e a mezzo fax, della duplicazione attraverso fotocopie, del trasporto documenti e posta e del trasferimento fra i diversi uffici della scuola di domande, documenti ed elenchi contenenti dati personali. Ai **Collaboratori Incaricati** spetta anche la vigilanza sui locali in cui avviene il trattamento di dati personali al fine di impedire l'intrusione da parte di persone non autorizzate, nonché Impedire il danneggiamento, la manomissione la sottrazione, la distruzione o la copia di dati nei locali che gli sono stati affidati in custodia da parte di persone non autorizzate secondo quanto stabilito dal Responsabile del Trattamento. I Collaboratori debbono, infine, identificare e verificare l'autorizzazione all'accesso ai locali dei soggetti ammessi dopo l'orario di chiusura degli uffici.

C. **Il Titolare del trattamento** in riferimento **all'Area Alunni** ha ritenuto opportuno di designare i **"DOCENTI"** (inclusi gli assistenti alla didattica, assistenti tecnici e personale di sostegno) quali **Incaricati del trattamento dei dati** degli alunni qualora necessari allo svolgimento della funzione di

istruzione ed assistenza scolastica, ricomprendendovi, altresì, anche docenti esterni incaricati ufficialmente di funzioni all'interno dell'Istituto Scolastico (esami, corsi, concorsi e attività integrative). Peraltro ogni dipendente che cessa di appartenere alle categorie in questione, in quanto non più in servizio nell'Istituto, deve cessare automaticamente dalla funzione di ***Incaricato del trattamento dei dati*** degli alunni, mentre ogni nuovo dipendente che entra a far parte di queste categorie assume automaticamente la funzione di ***Incaricato del trattamento dei dat***i. Questi incaricati sono autorizzati a trattare tutti i dati personali, ivi compresi quelli sensibili e giudiziari, con cui entrino comunque in contatto nell'ambito dell'espletamento dell'attività di loro competenza e in particolare di poter consultare il fascicolo personale degli alunni e qualunque documento necessario per l'attività istituzionale. E' stata, altresì, prospettata la necessità di nominare **Responsabili delle copie di sicurezza** onde evitare la perdita o la distruzione dei dati e provvedere al ricovero periodico degli stessi con copie di sicurezza**,** assicurandosi della qualità delle copie di sicurezza dei dati e della loro conservazione in luogo adatto e sicuro e provvedere, altresì, a conservare con la massima cura e custodia i dispositivi utilizzati per le copie di sicurezza, impedendo l'accesso agli stessi dispositivi da parte di personale non autorizzato-

3. *Nomine ed Incarichi*

- **Titolare del trattamento:**

Il Dirigente Scolastico Prof.ssa Maria Canosa

- **Responsabile del trattamento dei dati:**

Il Direttore dei Servizi Generali e Amministrativi Sig. Nicolina Piluso

- **Responsabile della sicurezza informatica:**

la Ditta Assistenza Scuola S.r.l.s. Via Punta Palizzi, 6 00122 ROMA,
Partita IVA 15064481003

- **Custode delle password:**

Il Direttore dei Servizi Generali e Amministrativi (vedi sopra)

- **Incaricati del trattamento dei dati**:

come da allegati

- **Incaricato dell'assistenza e della manutenzione degli strumenti**

elettronici/informatici:

la Ditta Assistenza Scuola S.r.l.s. Via Punta Palizzi, 6 00122 ROMA, Partita IVA 15064481003

4. Analisi dei Rischi, Vulnerabilità, Pericoli

L'analisi dei rischi consente di acquisire consapevolezza e visibilità sul livello di esposizione al rischio del patrimonio informativo e avere una mappa preliminare dell'insieme delle possibili contromisure di sicurezza da realizzare. L'analisi dei rischi consiste nella:

- individuazione di tutte le risorse del patrimonio informativo (dati, obbligatori per disposizione di legge, relativi al personale dipendente in forza e cessato; elenco alunni; dati/informazioni di fornitori e clienti nei limiti necessari ad ottemperare alle disposizioni fiscali e contabili in vigore; documenti cartacei; hardware; software; apparecchiature di comunicazione; servizi; immagine dell'Istituto);
- identificazione dei rischi cui tali risorse sono sottoposti;
- identificazione delle vulnerabilità;
- definizione delle contromisure;
- dati personali.

La classificazione dei **DATI** in funzione dell'analisi dei rischi è la seguente:

•***DATI ANONIMI*,** ovvero la classe di dati a minore rischio, per la quale non sono previste particolari misure di sicurezza se non quelle di tutela del patrimonio informativo dell'Istituto da perdite e/o danneggiamenti;

•***DATI PERSONALI***:

a) ***DATI PERSONALI SEMPLICI***, ovvero la classe di dati a rischio intermedio

b) ***DATI PERSONALI SENSIBILI/GIUDIZIARI***, ovvero la classe di dati ad alto rischio;

c) ***DATI PERSONALI SANITARI***, ovvero la classe di dati a rischio altissimo.

5. Individuazione delle risorse da proteggere

le risorse da proteggere sono:

1. Le Banche Dati dell'Istituto di cui al punto **1.**

2. Archivio protocollo con i dati relativi alla corrispondenza spedita e ricevuta;

3. I documenti cartacei;
4. L'hardware;
5. Il software;
6. Le apparecchiature di comunicazione;
7. L'immagine dell'Istituzione Scolastica.

4.1 Individuazione dei Pericoli

Nella tabella seguente sono elencati gli eventi potenzialmente in grado di determinare danno a tutte o parte delle risorse indicate nell'articolo 5.

Rischi	Deliberato	Accidentale	Ambientale
Terremoto			X
Inondazione		X	X
Uragano			X
Fulmine			X
Bombardamento	X	X	
Fuoco	X	X	
Uso di armi		X	
Danno volontario	X		
Interruzione di corrente		X	
interruzione di acqua		X	
Interruzione di aria condizionata	X	X	
Guasto hardware		X	
Linea elettrica instabile		X	X
Temperatura e umidità eccessive			X
Polvere			X
Radiazioni elettromagnetiche		X	
Scariche elettrostatiche		X	
Furto	X		
Uso non autorizzato dei supporti di memoria	X		
Deterioramento dei supporti di memoria		X	
Errore del personale operativo		X	
Errore di manutenzione		X	
Masquerading dell'identificativo dell'utente	X		

Uso illegale di software	X	X	
Software dannoso		X	
Esportazione/importazione illegale di software	X		
Accesso non autorizzato alla rete	X		
Uso della rete in modo non autorizzato	X		
Guasto tecnico di provider di rete		X	
Danni sulle linee	X	X	
Errore di trasmissione		X	
Sovraccarico di traffico	X	X	
Intercettazione (Eavesdropping)	X		
Infiltrazione nelle comunicazioni	X		
Analisi del traffico		X	
Indirizzamento non corretto dei messaggi		X	
Reindirizzamento dei messaggi	X		
Guasto dei servizi di comunicazione	X	X	
Mancanza di personale		X	
Errore dell'utente	X	X	
Uso non corretto delle risorse	X	X	
Guasto software	X	X	
Uso di software da parte di utenti non autorizzati	X	X	
Uso di software in situazioni non autorizzate	X	X	
Rischi	**Deliberato**	**Accidentale**	**Ambientale**

4.2 Individuazione delle Vulnerabilita'

Nelle tabelle seguenti sono elencate le vulnerabilità del sistema informatico che possono essere potenzialmente sfruttate qualora si realizzasse uno dei pericoli indicati al punto 5.

Infrastruttura	Hardware	Comunicazioni
Mancanza di protezione fisica dell'edificio (porte finestre ecc.)	Mancanza di sistemi di rimpiazzo	Linee di comunicazione non protette
Mancanza di controllo di accesso	Suscettibilità a variazioni di tensione	Giunzioni non protette

Linea elettrica instabile	Suscettibilità a variazioni di temperatura	Mancanza di autenticazione
Ubicazione suscettibile ad allagamenti	Suscettibilità a umidità, polvere, sporcizia	Connessioni a linea pubblica non protette
	Suscettibilità a radiazioni elettromagnetiche	Mancanza di prova di ricezione/invio
	Manutenzione insufficiente	Presenza di linee dial-up (con modem)
	Carenze di controllo di configurazione (update/upgrade dei sistemi)	Traffico sensibile non protetto

Documenti cartacei	Software	Personale
Locali documenti non protetti	Interfaccia uomo-macchina complicata	Mancanza di personale
Carenza di precauzioni nell'eliminazione	Mancanza di identificazione / autenticazione	Mancanza di supervisione degli esterni
Non controllo delle copie	Mancanza del registro delle attività (log)	Formazione insufficiente sulla sicurezza
	Errori noti del software	Mancanza di consapevolezza
	Tabelle di password non protette	Uso scorretto di hardware/software
	Scorretta allocazione dei diritti di accesso	Carenza di monitoraggio
	Carenza di controllo nel caricamento e uso di software	Mancanza di politiche per i mezzi di comunicazione
	Permanenza di sessioni aperte	Procedure di reclutamento inadeguate
	Carenza di controllo di configurazione	
	Carenza di documentazione	
	Incuria nella dismissione di supporti riscrivibili	

4.3 Individuazione dei Pericoli cui sono sottoposte le Risorse Hardware

I principali pericoli che possono incombere sulle risorse hardware sono:

1. malfunzionamenti dovuti a guasti;
2. malfunzionamenti dovuti a eventi naturali quali terremoti, allagamenti, incendi;
3. malfunzionamenti dovuti a blackout ripetuti ed in genere a sbalzi eccessivi delle linee di alimentazione elettrica;
4. malfunzionamenti dovuti a sabotaggi, furti, intercettazioni (apparati di comunicazione).

4.4 Individuazione dei Pericoli cui sono sottoposte le Risorse connesse in rete

I principali pericoli alle risorse connesse in rete possono provenire dall'interno del Teatro, dall'esterno o da una combinazione interno/esterno e sono relative:

1. all'utilizzo della LAN (pericoli interni);
2. ai punti di contatto con il mondo esterno attraverso Internet (pericoli esterni);
3. allo scaricamento di virus e/o trojan per mezzo di posta elettronica e/o alle operazioni di download eseguite tramite il browser (interni/esterni).

In riferimento a quest'ultimo punto si ritiene opportuno evidenziare le tecniche più in uso:

- ***IP SPOOFING***, l'autore dell'attacco sostituisce la propria identità a quella di un utente legittimo del sistema. Viene fatto non per generare intrusione in senso stretto, ma per effettuare altri attacchi. Lo spoofing si manifesta come attività di "falsificazione" di alcuni dati telematici, come ad esempio di un indirizzo IP o dell'indirizzo di partenza dei messaggi di posta elettronica;
- ***PACKET SNIFFING***, apprendimento di informazioni e dati presenti sulla Rete o su un sistema, tramite appositi programmi. Consiste in un'operazione di intercettazione passiva delle comunicazioni di dati ed informazioni che transitano tra sistemi informatici. In particolare, un aggressore (hacker) può essere in grado di intercettare transazioni di varia natura (password, messaggi di posta elettronica, etc.). L'intercettazione illecita avviene con l'ausilio degli sniffer, strumenti che catturano /e informazioni in transito per il punto in cui sono installati. Gli sniffer possono anche essere installati su di un computer di un soggetto inconsapevole, in questo caso è possibile che prima dell'installazione dello sniffer, la macchina "obiettivo" sia

stata oggetto di un precedente attacco e sia di fatto controllata dall'hacker;

- ***PORT SCANNING***, serie programmata di tentativi di accesso diretti a evidenziare, in base alle "risposte" fornite dallo stesso sistema attaccato, le caratteristiche tecniche del medesimo (e le eventuali vulnerabilità), al fine di acquisire gli elementi per una "intrusione". Trattasi di un vero e proprio studio delle vulnerabilità di un sistema; gli amministratori dei sistemi eseguono spesso questa funzione allo scopo di verificare la funzionalità del medesimo;

- ***HIGHJACKING***, intrusione in una connessione di Rete in corso. In questo modo si colpiscono principalmente i flussi di dati che transitano nelle connessioni point to point. In sostanza l'hacker, simulando di essere un'altra macchina al fine di ottenere un accesso, si inserisce materialmente nella transazione, dopo averne osservato attentamente il flusso. L'operazione è complessa e richiede elevate capacità e rapidità d'azione;

- ***SOCIAL ENGINEERING,*** apprendimento fraudolento da parte degli utenti di sistemi di informazioni riservate sulle modalità di accesso a quest'ultimo;

- ***BUFFER OVERFLOW***, azioni che tendono a sfruttare eventuali anomalie e difetti di applicazioni che installate in alcuni sistemi operativi, forniscono le funzionalità di "amministratore del sistema", consentendo il controllo totale della macchina. L'hacker, dunque, con tale azione va a sconvolgere la funzionalità di tali programmi, prendendo il controllo della macchina vittima;

- ***SPAMMING,*** saturazione di risorse informatiche a seguito dell'invio di un elevato numero di comunicazioni tali da determinare l'interruzione del servizio. Ad esempio l'invio di molti messaggi di posta elettronica con allegati provoca, come minimo, la saturazione della casella e la conseguente non disponibilità a ricevere ulteriori (veri) messaggi;

- ***PASSWORD CRACKING***, sono programmi che servono per decodificare le password, una volta entrati in possesso del/dei file delle parole d'ordine;

- ***TROJAN,*** appartengono alla categoria dei virus, di solito sono nascosti in file apparentemente innocui che vengono inconsciamente attivati dall'utente. Permettono, una volta attivati, di accedere incondizionatamente al sistema;

- ***WORM,*** appartengono alla categoria dei virus e sono programmi che si replicano attraverso i computer connessi alla rete. In genere consumano una gran quantità di risorse di rete (banda) e di conseguenza possono essere utilizzati per gli attacchi DOS (denial of service) in cui si saturano le risorse di un server o di una rete producendo una condizione di non disponibilità (non funzionamento);

- ***LOGIC BOMB***, appartengono alla categoria dei virus e sono programmi che contengono a/ proprio interno una funzione diretta a danneggiare o impedire il funzionamento del sistema, in grado di attivarsi autonomamente a distanza di tempo dall'attivazione;
- ***MALWARE E MMC (MALICIOUS MOBILE CODE***), costituiscono la macrocategoria di codici avente come effetto il danneggiamento e l'alterazione del funzionamento di un sistema informativo e/o telematico. In tale categoria sono incluse anche alcune forme di codice ad alta diffusione, quali i virus, i worms ed i trojan horses;
- ***DOS (DENIAL OF SERVICE***), attacco che mira a saturare le risorse di un servizio, di un server o di una rete;
- ***DDOS (DISTR1BUTED DENIAL OF SERVICE***), attacco ripetuto e distribuito che mira a saturare le risorse di un servizio, di un server o di una rete.

4.5 Individuazione dei Pericoli cui sono sottoposti i Dati trattati

I principali pericoli sui dati trattati sono:

1. accesso non autorizzato agli archivi contenenti le informazioni riservate da parte di utenti interni e/o esterni;
2. modifiche accidentali agli archivi da parte di utenti autorizzati.

4.6 Individuazione dei Pericoli cui sono sottoposti i Supporti di memorizzazione

I principali pericoli sui supporti di memorizzazione sono:

- distruzione e/o alterazione a causa di eventi naturali;
- imperizia degli utilizzatori;
- sabotaggio;
- deterioramento nel tempo (invecchiamento dei supporti);
- difetti di costruzione del supporto di memorizzazione che ne riducono la vita media;
- evoluzione tecnologica del mercato che rende in breve tempo obsoleti alcuni tipi di supporti.

5. Individuazione delle Contromisure

In questa parte del documento vengono descritte le misure adottate per annullare o limitare le vulnerabilità e contrastare i **PERICOLI**. Per misura viene inteso lo specifico intervento di carattere fisico, procedurale ed elettronico/informatico posto in essere per prevenire, contrastare o ridurre gli effetti relativi ad una specifica minaccia, nonché per assicurare il livello minimo di protezione.

5.1 Contromisure di carattere fisico e procedurale

Contro i rischi di intrusione i locali sono dotati di impianto di allarme a sensori infrarossi, attivabile mediante digitazione di un codice in possesso del personale dipendente. L'attivazione di detto sistema di allarme avviene al termine dell'orario di lavoro.

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 stesso. L'ubicazione di stampanti ed apparecchio telefax tradizionale non consente ad estranei di leggere od asportare eventualmente documenti non ancora prelevati dal personale. Il personale amministrativo, incaricato del trattamento, ha ricevuto le opportune istruzioni per la tutela e la protezione dei dati in formato cartaceo e dei dispositivi informatici attraverso i quali avviene il trattamento dei dati personali.
L'accesso ai locali in cui avviene il trattamento e la custodia di dati personali è vigilato dai Collaboratori Scolastici cui è assegnato il compito di impedire l'intrusione da parte di persone non autorizzate e di identificare e quindi verificare l'autorizzazione all'accesso ai locali dei soggetti ammessi dopo l'orario di chiusura degli uffici. In riferimento ai supporti cartacei, sono state impartite dettagliate istruzioni per la protezione dei quali

- 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;

- eventuali rubriche telefoniche in utilizzo su supporto cartaceo debbono essere richiuse dopo la consultazione ed il primo foglio delle rubriche stesse, leggibile dall'esterno, non deve contenere alcun dato (praticamente il primo foglio funge da copertina);
- è permesso l'accesso ai soli dati strettamente necessari allo svolgimento delle proprie mansioni;
- è fatto divieto di fotocopiare/scannerizzare documenti senza l'autorizzazione del Responsabile del trattamento;
- massima attenzione dovrà essere posta ai documenti che si trovano in locali accessibili al pubblico;
- è fatto divieto di esportare documenti o copie dei medesimi all'esterno. Tutti i documenti cartacei devono essere gestiti in modo da ridurre al minimo i tempi di permanenza al di fuori degli archivi o degli armadi o dei contenitori in dotazione alle unità operative;
- l'accesso agli archivi è consentito al personale a ciò espressamente autorizzato in via permanente od occasionale;
- E' fatto divieto di fotocopiare, passare allo scanner e comunque riprodurre documenti senza l'autorizzazione del Responsabile del trattamento;
- gli archivi devono essere mantenuti costantemente chiusi, compatibilmente con le esigenze di servizio. Le copie dei documenti e/o scansioni vanno trattate, con riferimento alla tutela dei dati personali in esse contenuti, con la medesima diligenza riservata agli originali;
- gli Incaricati che possono essere trattati dati sensibili o giudiziari, hanno ricevuto dettagliate istruzioni onde porre massima attenzione al rispetto delle disposizioni precedenti. Essi, inoltre, dovranno limitare al minimo indispensabile la giacenza della documentazione al di fuori degli armadi o contenitori muniti di serratura; controllare con particolare rigore l'accesso ai propri archivi, autorizzare e registrare eventuali accessi negli uffici compiuti al di fuori degli usuali orari di lavoro;
- Gli Incaricati nominati sono responsabili della riservatezza dei registri in cui sono annotati dati comuni e particolari. Fuori dall'orario di servizio, e comunque quando non necessario all'espletamento dei compiti, i registri

devono essere conservati negli appositi armadi/cassetti chiusi a chiave; una chiave di riserva è mantenuta con le dovute cautele dal Responsabile del trattamento in armadietto chiuso a chiave;

- il protocollo riservato, accessibile solo al Titolare e al Responsabile del trattamento è conservato nell' ufficio del Dirigente Scolastico;
- la responsabilità del controllo sui documenti stampati è del Responsabile del trattamento. Il materiale cartaceo destinato allo smaltimento dei rifiuti deve essere ridotto in frammenti: all'uopo vi è in dotazione apposito macchinario distruggi documenti
- l'ingresso in locali ad accesso controllato da parte di dipendenti o estranei per operazioni di pulizia o di manutenzione avviene solo se i contenitori dei dati sono chiusi a chiave e i computer sono spenti oppure se le operazioni si svolgono alla presenza dell'Incaricato del trattamento dei dati.

5.2 Contromisure di carattere elettronico/informatico

In riferimento alle misure di carattere elettronico/informatico sono state impartite dettagliate istruzioni per la protezione quali:

- Utilizzo di server con configurazioni di ridondanza;
- presenza di gruppi di continuità elettrica per il server;
- attivazione di un sistema di backup automatizzato con periodicità settimanale e una copia storica ad un mese. Le copie di backup realizzate giornalmente debbono essere conservate in un armadio di ferro chiuso a chiave possibilmente ignifugo;
- firewall ridondante che protegge la rete dagli accessi indesiderati attraverso internet; la navigazione degli utenti è filtrata ed è bloccata la consultazione dei siti i cui URL appartengono alle sotto elencate categorie:

	Categorie
Adult/Sexually Explicit	Siti per adulti/Sesso esplicito
Chat	Chat
Criminal Skills	Siti riguardanti lo criminalità
Drugs, Alcohol & Tabacco	Droga, Alcool e Tabacco
Food Drink	Siti riguardanti la ristorazione
Gambling	Scommesse

Games	Giochi
Glamour & Intimate Apparel	Biancheria ed Intimo
Hacking	Pirateria informatica
Hate Speech	Incitamento all'odio
Hobbies & Recreation	Hobbies e divertimento
Kid's Sites	Siti con contenuti su minori
Motor Vehicles	Siti riguardanti i motori
Personals & Dating	Chat con informazioni personali (ad esempio Facebook)
Religion	Siti riguardanti argomenti religiosi
Sex Education	Educazione sessuale
Sports	Sports
Violence	Siti riguardanti argomenti di violenza
Weapons	Armi

- definizione delle regole per la gestione di password sui sistemi operativi

    a. l'accesso al sistema informativo degli incaricati del trattamento dei dati personali è permesso per mezzo di un codice identificativo personale (user-id) e password personale;

    b. al primo accesso, la password ottenuta dal Responsabile del Servizio Informatico deve essere cambiata;

    c. la password deve essere costituita da una sequenza di minimo otto caratteri alfanumerici e non deve essere facilmente individuabile;

    d. deve successivamente essere cambiata almeno ogni sei mesi;

    a. è segreta e non deve essere comunicata ad altri;

    b. va custodita con diligenza e riservatezza;

    c. l'utente deve sostituire la password, nel caso ne accertasse la perdita;

    d. le password verranno automaticamente disattivate dopo tre mesi di non utilizzo a cura del Servizio Informatico;

- in caso di manutenzione straordinaria possono essere comunicate, qualora necessario, dall'amministratore di sistema al tecnico/sistemista addetto alla manutenzione le credenziali di **autenticazione di servizio**. Al termine delle operazioni di manutenzione l'amministratore di sistema deve ripristinare **nuove credenziali** di autenticazione;
- la rete è protetta da un sistema antivirus e antispyware che distribuisce gli aggiornamenti ai server e ai client sulla rete in automatico;
- definizione delle regole di comportamento per minimizzare i rischi da virus:
    a. limitare lo scambio fra computer di supporti rimovibili (floppy, cd, pen drive, zip) contenenti file con estensione EXE, COM, OVR, OVL, SYS, DOC, XLS;
    b. controllare (scansionare con un antivirus aggiornato) qualsiasi supporto di provenienza sospetta prima di operare su uno qualsiasi dei file in esso contenuti;
    c. evitare l'uso di programmi shareware e di pubblico dominio se non se ne conosce la provenienza, ovvero divieto di "scaricare" dalla rete internet ogni sorta di file, eseguibile e non. La decisione di "scaricare" può essere presa solo dal Responsabile del Servizio Informatico;
    d. disattivare gli Activex e il download dei file per gli utenti del browser Internet Explorer;
    e. disattivare la creazione di nuove finestre ed il loro ridimensionamento e impostare il livello di protezione su "chiedi conferma" (il browser avvisa quando uno script cerca di eseguire qualche azione);
    f. attivare la protezione massima per gli utenti del programma di posta Outlook Express al fine di proteggersi dal codice html di certi messaggi e-mail (buona norma è visualizzare e trasmettere messaggi in formato testo poiché alcune pagine web, per il solo fatto di essere visualizzate, possono infettare il computer);

g. non aprire gli allegati di posta se non si è certi della loro provenienza, e in ogni caso analizzarli con un software antivirus. Usare prudenza anche se un messaggio proviene da un indirizzo conosciuto (alcuni virus prendono gli indirizzi dalle mailing list e dalla rubrica di un computer infettato per inviare nuovi messaggi "infetti");
h. non cliccare mai su di un link presente in un messaggio di posta elettronica da provenienza sconosciuta, (in quanto potrebbe essere falso e portare a un sito-truffa);
i. non utilizzare le chat;
j. seguire scrupolosamente le istruzioni fornite dal sistema antivirus nel caso in cui tale sistema antivirus abbia scoperto tempestivamente il virus (in alcuni casi esso è in grado di risolvere il problema, in altri chiederà di eliminare o cancellare il file infetto);

- definizione delle regole di comportamento in caso di sistemi danneggiati seriamente da virus.

L'Amministratore di Sistema procede a reinstallare il sistema operativo, i programmi applicativi ed i dati seguendo la procedura indicata:

a. formattare l'Hard Disk, definire le partizioni e reinstallate il Sistema Operativo;
b. installare il software antivirus, verificare e installare immediatamente gli eventuali ultimi aggiornamenti;
c. reinstallare i programmi applicativi a partire dai supporti originali;
d. effettuare una scansione per rilevare la presenza di virus nelle copie dei dati;
e. effettuare il RESTORE dei soli dati a partire da una recente copia di BACKUP;
f. NESSUN PROGRAMMA ESEGUIBILE DEVE ESSERE RIPRISTINATO DALLA COPIA DI BACKUP, potrebbe essere infetta;
g. ricordare all'utente di prestare particolare attenzione al manifestarsi di nuovi malfunzionamenti nel riprendere il lavoro di routine;

- separazione fisica della rete della Biglietteria da quella della Fondazione, quest'ultima, in quest'anno, ha subito un ampliamento nella zona antecedente l'infermeria al secondo ordine.

5.3 Incident Response e Ripristino

Tutti gli incaricati del trattamento dei dati devono avvisare tempestivamente l'Amministratore di Sistema o il responsabile del trattamento dei dati, nel caso in cui constatino le seguenti anomalie:

1. discrepanze nell'uso degli user-id;
2. modifica e sparizione di dati;
3. cattive prestazioni del sistema (così come percepite dagli utenti);
4. irregolarità nell'andamento del traffico;
5. irregolarità nei tempi di utilizzo del sistema;
6. quote particolarmente elevate di tentativi di connessione falliti.

In caso di incidente sono considerate le seguenti priorità:

1. evitare danni diretti alle persone;
2. proteggere l'informazione sensibile o proprietaria;
3. evitare danni economici;
4. limitare i danni all'immagine della Fondazione;
5. garantita l'incolumità fisica alle persone procedendo ad isolare l'area contenente il sistema oggetto dell'incidente, ad isolare il sistema compromesso dalla rete e successivamente a spegnere correttamente il sistema.

Una volta spento il sistema oggetto dell'incidente non deve più essere riacceso.

5.4 Piano di formazione

La formazione degli incaricati viene effettuata all'ingresso in servizio e all'installazione di nuovi strumenti per il trattamento dei dati.

Le finalità della formazione sono:

1. sensibilizzare gli incaricati sulle tematiche di sicurezza, in particolar modo sui rischi e sulle responsabilità che riguardano il trattamento dei dati personali;

2. proporre buone pratiche di utilizzo sicuro della rete;

3. riconoscere eventuali anomalie di funzionamento dei sistemi (hardware e software) correlate a problemi di sicurezza.

Il piano prevede inoltre la pubblicazione di normativa ed ordini di servizio.

6. Norme per il Personale

Tutti i dipendenti concorrono alla realizzazione della sicurezza, pertanto devono proteggere le risorse loro assegnate per lo svolgimento dell'attività lavorativa con gli strumenti, nel rispetto di quanto stabilito nel presente Documento e dall'allegato N° 1 "Regolamento per l'uso della Rete Informatica..”

7. Smaltimento Rifiuti Apparecchiature Elettroniche e Misure di Sicurezza dei Dati Personali

Viste le disposizioni del garante della privacy contenute nel provvedimento n° 287/2008 s.m.i. in riferimento ai rifiuti delle apparecchiature *“Rifiuti di apparecchiature elettroniche e misure di sicurezza dei dati personali”*, per lo smaltimento dei PC in disuso si sono date disposizioni di avvalersi di tecnico qualificato per:

a) demagnetizzare l’hard disk;
b) cancellare i files presenti nell’hard disk utilizzando ad esempio i programmi che provvedono a scrivere ripetutamente nelle aree del disco precedentemente occupate dalle informazioni eliminate sequenze casuali di cifre binarie in modo da ridurre al minimo le probabilità di recupero delle informazioni;
c) distruggere fisicamente il supporto di memoria

Può essere anche una buona regola per ogni PC eliminato redigere apposito verbale.

PARTE SPECIALE SECONDA

GLI ALLEGATI

1. **Regolamento Generale per l'uso della Rete Informatica**
   (Articoli 33-36 Del D.Lgs. Num. 196/2003 S.M.I.);

2. **Disciplinare Interno per l'uso Telefoni, Fax , Internet e Posta Elettronica**

3. **Regolamento relativo alla identificazione e alle modalità di trattamento dei dati sensibili e giudiziari del Personale Scolastico e degli Alunni;**

   2a. Informativa ex art. 13 D.Lgs. N. 196/2003 s.m.i. per il Trattamento dei Dati del personale dipendente;
   2b. Acquisizione del consenso del soggetto interessato al Trattamento dei Dati ai sensi del D.L.Vo 196/2003 s.m.i.;
   2c. Modulo per la richiesta di accesso al Trattamento.

ALLEGATO 1.

REGOLAMENTO GENERALE PER L'USO DELLA RETE INFORMATICA

(articoli 33-36 del d.lgs. num. 196/2003 s.m.i.)

art. 1 Principi Generali

Il presente regolamento disciplina le modalità di accesso e di uso della rete informatica e telematica dell'Istituto Nelson Mandela e dei servizi che, tramite la stessa rete (connessa alla rete Internet), è possibile ricevere o offrire.
Tutti i dipendenti concorrono alla realizzazione della sicurezza, pertanto devono proteggere le risorse loro assegnate per lo svolgimento dell'attività lavorativa, nel rispetto di quanto stabilito nel presente documento.
Gli utenti per garantire l'integrità dei sistemi e delle relative risorse, in osservanza delle leggi, norme e obblighi contrattuali, consapevoli delle potenzialità offerte dagli strumenti informatici e telematici, si impegnano ad agire con responsabilità e a non commettere violazioni aderendo a un principio di autodisciplina.
Il posto di lavoro costituito da personal computer viene consegnato completo di quanto necessario per svolgere le proprie funzioni, pertanto **è proibito modificarne ubicazione e configurazione**.
Il software installato sui personal computer è quello necessario per lo svolgimento delle specifiche attività lavorative di ogni singolo utente. **E' pertanto proibito installare qualsiasi programma**.
Ogni utente è responsabile dei dati memorizzati nel proprio personal computer e del loro backup. Per questo motivo è tenuto ad effettuare la copia di questi dati regolarmente al massimo con cadenza settimanale, secondo indicazioni impartite dall'Amministratore di Sistema su delega del titolare del trattamento.

art. 2 Abusi e Attivita' Vietate

E vietato ogni tipo di abuso.
In particolare è vietato:

- **A.** usare la rete in modo difforme da quanto previsto dalle leggi penali, civili e amministrative e da quanto previsto dal presente regolamento;
- **B.** utilizzare la rete per scopi incompatibili con l'attività istituzionale della Fondazione;
- **C.** utilizzare una password a cui non si è autorizzati;
- **D.** cedere a terzi codici personali (USER ID e PASSWORD) di accesso al sistema, o a software che gestisce dati;
- **E.** conseguire l'accesso non autorizzato a risorse di rete interne o esterne a quella dell'Istituto;
- **F.** violare la riservatezza di altri utenti o di terzi;
- **G.** agire deliberatamente con attività che influenzino negativamente la regolare operatività della rete e ne restringano l'utilizzabilità e le prestazioni per altri utenti;
- **H.** agire deliberatamente con attività che distraggano risorse;
- **I.** fare o permettere ad altri trasferimenti non autorizzati di informazioni (software, basi dati, ecc.);
- **J.** installare o eseguire deliberatamente o diffondere su qualunque computer e sulla rete, programmi destinati a danneggiare o sovraccaricare i sistemi o la rete (p.e. virus, cavalli di troia, worms, spamming della posta elettronica, programmi di file sharing - p2p);
- **K.** installare o eseguire deliberatamente programmi software non autorizzati e non compatibili con le attività istituzionali;
- **L.** cancellare, disinstallare, copiare, o asportare deliberatamente programmi software per scopi personali;
- **M.** installare deliberatamente componenti hardware non compatibili con le attività istituzionali;
- **N.** danneggiare deliberatamente o asportare componenti hardware;
- **O.** utilizzare le risorse hardware e software e i servizi disponibili per scopi personali;
- **P.** utilizzare le caselle di posta elettronica della Fondazione per scopi personali e/o non istituzionali;
- **Q.** utilizzare la posta elettronica con le credenziali di accesso di altri utenti;
- **R.** utilizzare la posta elettronica inviando e ricevendo materiale che violi le leggi;
- **S.** utilizzare l'accesso ad Internet per scopi personali;
- **T.** accedere direttamente ad Internet con modem collegato al proprio Personal Computer se non espressamente autorizzati e per particolari motivi tecnici;
- **U.** connettersi ad altre reti senza autorizzazione;
- **V.** monitorare o utilizzare qualunque tipo di sistema informatico o elettronico per controllare le attività degli utenti, leggere copiare o cancellare file e software di

altri utenti, senza averne l'autorizzazione esplicita;

W. usare l'anonimato o servirsi di risorse che consentano di restare anonimi sulla rete;

X. inserire o cambiare la password del bios, se non dopo averla espressamente comunicata all'amministratore di sistema e essere stati espressamente autorizzati;

Y. abbandonare il posto di lavoro lasciandolo incustodito o accessibile.

art. 3 Attività Consentite

E' consentito all'**Amministratore di Sistema**:

1. monitorare o utilizzare qualunque tipo di sistema informatico o elettronico per controllare il corretto utilizzo delle risorse di rete, dei client e degli applicativi, per copiare o rimuovere file e software, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati;
2. creare, modificare, rimuovere o utilizzare qualunque password, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati. L'amministratore darà comunicazione dell'avvenuta modifica all'utente;
3. rimuovere programmi software, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati;
4. rimuovere componenti hardware, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati.

Art. 4 Soggetti che possono accedere alla rete

Hanno diritto ad accedere alla rete dell'Istituto:

A. tutti i dipendenti, le ditte fornitrici di software per motivi di manutenzione e limitatamente alle applicazioni di loro competenza;
   a. L'accesso agli incaricati ed agli addetti alla manutenzione è possibile solo in seguito ad autorizzazione del Responsabile del Trattamento dei Dati o dell'Amministratore di Sistema;
   b. tutte le operazioni di manutenzione che sono effettuate on-site avvengono con la supervisione del Responsabile del Trattamento, o dell'Amministratore di Sistema;

B. collaboratori esterni impegnati nelle attività istituzionali per il periodo di collaborazione.

L'accesso alla rete è assicurato compatibilmente con le potenzialità delle attrezzature.
L'accesso agli applicativi è consentito agli utenti che, per motivi di servizio, ne devono fare uso.
L'amministratore di sistema può regolamentare l'accesso alla rete di determinate categorie di utenti, quando questo è richiesto da ragioni tecniche.

art.5 Modalità' di accesso alla rete e agli applicativi

Qualsiasi accesso alla rete ed agli applicativi viene associato ad una persona fisica cui collegare le attività svolte utilizzando il codice utente. L'utente che ottiene l'accesso alla rete ed agli applicativi si impegna ad osservare le presenti norme disciplinanti le attività ed i servizi che si svolgono via rete e si impegna a non commettere abusi e a non violare i diritti degli altri utenti e dei terzi, assumendosi la totale responsabilità delle attività svolte tramite la rete.

art.6 Utilizzo di INTERNET

La consultazione di siti web da parte del lavoratore o l'utilizzo di posta elettronica è regolamentato dall' apposito Disciplinare Interno cui ci si riporta.
Giova, peraltro, immediatamente evidenziare :

1. la responsabilità civile disciplinata dall'art. 2050 del Codice Civile e art. 15 D.Lgs. 196/03 "***chi cagiona danno ad altri per effetto del trattamento dei dati personali tenuto a risarcire il danno, a meno che non provi di aver adottato tutte le misure idonee per evitarlo***";
2. la sanzione penale che colpisce chi, essendovi tenuto, omette di adottare le misure di sicurezza (art. 169 del D.Lgs. 196/03 s.m.i.), è pari all'arresto fino a due anni o ad ammenda da 10mila a 50mila euro, ma con estinzione del reato in caso di regolarizzazione entro 6 mesi dall'accertamento del reato e pagamento di somma determinata dal Garante.

art.7 SANZIONI

In caso di abuso, a seconda della gravità del medesimo, e fatte salve ulteriori conseguenze di natura penale, civile e amministrativa, possono essere comminate le sanzioni disciplinari previste dalla normativa vigente in materia e dal Disciplinare Interno, oltre all'eventuale risarcimento del danno cagionato.

ALLEGATO 2.

DISCIPLINARE INTERNO PER L'USO TELEFONI, INTERNET E POSTA ELETTRONICA

SOMMARIO

PREMESSE

Il Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione di dati personali " impone comportamenti tali da assicurare a chiunque il diritto alla protezione dei dati personali che lo riguardano: a tal fine L'Istituto ha adottato il "Documento sulla Sicurezza Informatico".

Inoltre non devesi preterire che il Dipartimento della Funzione Pubblica ha emesso la Direttiva n° 02/09 con la quale richiama l'attenzione sulla Deliberazione 13/2007 (" Lavoro: le linee guida del Garante per Posta Elettronica e Internet") emanata dal Garante per la protezione dei dati personali ha emanato, in data 01.03.2007, contenente prescrizioni per Datori di lavoro di adottare la "misura necessaria", a garanzia dei lavoratori in riferimento all'utilizzo da parte di costoro della Posta Elettronica e della rete Internet.

Infine non è ultroneo qui ricordare che l'art. 10, comma 3, del "*Codice di comportamento dei dipendenti della pubbliche Amministrazioni "* dispone che " *il dipendente non utilizzi a fini privati materiale o attrezzature di cui dispone per ragioni d'ufficio*".

L'Istituto Nelson Mandela, nell'ottica doverosa di trasparenza e correttezza, al fine di assicurare il corretto espletamento delle funzioni dell'Ente e la liceità dell'attività svolta dai Lavoratori, emana il presente Disciplinare per regolamentare l'utilizzo della Posta Elettronica, del Fax mail, della rete Internet anche dei telefoni aziendali, ricomprendendo in essi quelli "fissi", i "cellulari", i "palmari".

Art. 1: Finalità

1. Le disposizioni dettate col Disciplinare sono dirette a proteggere gli interessi dell'Amministrazione e tutelare la riservatezza dei dati personali dei Lavoratori rispetto all'uso di: Posta Elettronica, Internet e telefoni aziendali ("fissi", "cellulari", "palmari").
2. A tal fine l'oggetto del presente disciplinare riguarda:

a) la modalità di utilizzo della Posta Elettronica, della rete Internet, dei telefoni "fissi", dei telefoni "cellulari", dei palmari da parte dei Lavoratori, così come qualificati al successivo art. 2;
b) le modalità con le quali vengono effettuati controlli sull'uso di questi strumenti.

Art. 2: Campo di applicazione del Disciplinare

1. Il presente Disciplinare si applica a tutti i Lavoratori:
a) dirigenti e dipendenti, a qualsiasi titolo inseriti nell'organizzazione scolastica, senza distinzione di ruolo e/o mansione.
b) collaboratori dell'Istituto, a prescindere dal rapporto contrattuale intrattenuto con la stessa.

Art. 3: Posta Elettronica, Internet e telefoni aziendali: considerazioni generiche sull'utilizzo

1. L'Istituto Nelson Mandela vuole essere un luogo di lavoro nel quale sia assicurata la tutela dei diritti, delle libertà fondamentali e della dignità dei Lavoratori, in nella consapevolezza della reciprocità dei diritti e dei doveri.
2. Le risorse informatiche e telematiche, messe a disposizione dall'Istituto, devono essere utilizzate in modo responsabile e ispirato ai principi di diligenza e correttezza per cui l'utilizzo improprio, da parte del Lavoratore, di **Posta Elettronica, Internet e telefoni aziendali**, può pregiudicare il regolare funzionamento delle installazioni tecniche nonchè compromettere interessi meritevoli di tutela e/o giuridicamente protetti, fra cui:

a) economie dei costi;
b) la capacità di memoria utilizzabile dei server o l'ampiezza di banda disponibile per il collegamento in rete;
c) sicurezza delle applicazioni e dei dati (disponibilità, integrità, confidenzialità);
d) produttività sul lavoro;
e) la reputazione o l'immagine dell' Istituto;
f) responsabilità oggettiva dell' Istituto, a mente dell'art. 2049 CC, derivante

da comportamenti illeciti dei propri dipendenti.

3. Per il lavoratore, i rischi derivanti dall'utilizzo di Posta Elettronica, Internet e telefoni aziendali, riguardano:

a) la protezione dei dati personali, propri e di terzi, poiché i predetti strumenti lasciano "tracce" del loro uso;
b) la possibilità che l'Istituto, in fase di eventuale legittimo controllo, venga a conoscenza di dati od opinioni personali del Lavoratore;
c) relativamente all'uso di Posta Elettronica e di Internet, l'introduzione di virus, worm, cavalli di Troia o installazioni di programmi estranei nel computer utilizzato dal Lavoratore, con conseguente perdita di tutti o parte dei file salvati sul medesimo computer.

Art. 4: Definizione degli strumenti di lavoro

La Posta Elettronica, l'accesso alla rete Internet, i telefoni aziendali ed i fax devono ritenersi normali strumenti di lavoro, forniti in dotazione dall'Istituto per lo svolgimento di attività lavorativa.

Art. 5: Uso dei telefoni "fissi" sul posto di lavoro

1. I telefoni "fissi" che l' Istituto mette a disposizione devono essere utilizzati in modo strettamente pertinente allo svolgimento dell'attività lavorativa, secondo un utilizzo appropriato, efficiente, corretto e razionale.
2. Solo in caso di particolare necessità e/o urgenza e previa autorizzazione del Dirigente Scolastico o del DSGA i Lavoratori possono utilizzare i telefoni "fissi" per motivi non attinenti l'attività lavorativa e, comunque, non in modo ripetuto o per periodi di tempo prolungati.
3. L'Istituto raccoglie i log files per analisi, anche di ordine statistico, dirette al perseguimento di finalità organizzative, produttive e di sicurezza.

I dati raccolti vengono conservati per il tempo strettamente necessario alle suddette analisi e finalità. In caso di anomalie riscontrate nelle modalità di utilizzo del telefono aziendale, si applicherà quanto previsto dal successivo art. 11 del presente disciplinare.

Art. 6: Uso dei Fax

1. All'utilizzo dei Fax dell'Istituto si applicano le disposizioni previste per l'utilizzo dei telefoni "fissi" di cui all'art. 5.
2. Per l'uso della posta elettronica di cui al successivo art. 9.

Art. 7: Accesso ad Internet

a. In via preliminare è opportuno richiamare quanto viene riportato nelle Linee Guida per la Sicurezza ICT delle Pubbliche Amministrazioni redatte deal Comitato Nazionale per l'Informatica nella Pubblica Amministrazione:

"Tutti i dipendenti dell'Amministrazione sono tenuti ad utilizzare i servizi di rete solo nell'ambito delle proprie mansioni di lavoro, secondo direttive circostanziate, essendo consapevoli che ogni accesso ad Internet può essere facilmente ricondotto alla persona che lo ha effettuato. Occorre quindi che i dipendenti si comportino con il massimo livello di professionalità quando operano in Internet, evitando eventi dannosi, anche al fine di non danneggiare l'immagine dell' Amministrazione".

Tanto premesso e considerato, altresì, che Internet è uno strumento di lavoro di utilità per l'Istituto, l'accesso ad Internet deve essere utilizzato in modo pertinente allo svolgimento dell'attività lavorativa, secondo un utilizzo appropriato, efficiente, corretto e razionale.

b. I lavoratori debbono utilizzare Internet per le specifiche finalità della propria attività così come disposto dall'art. 10 c.3 del Codice di Comportamento dei Dipendenti delle Pubbliche Amministrazioni;
c. I lavoratori, inoltre, non devono appesantire il traffico della rete con collegamenti particolarmente lunghi e complessi (es. download di file, connessioni a stazioni radio on line, applicazioni "peer to peer", chat, etc.) quando ciò non sia collegato allo svolgimento dell'attività lavorativa;
d. I lavoratori possono accedere ai siti Internet presenti nelle pagine Intranet, durante l'orario di lavoro, nel rispetto di quanto disposto al comma a. del presente articolo, essendo interesse e cura dell'Istituto proporre i siti Internet, anche di natura divulgativa, che possono essere utili all'espletamento dell'attività lavorativa;

e. I lavoratori non devono condurre attività commerciali di qualsiasi tipo a beneficio proprio e/o di terzi, attraverso l'accesso ad Internet, mediante uso di strumenti di proprietà dell'Istituto;

f. I lavoratori non devono, in alcun caso, accedere e navigare in siti web contenenti materiale pornografico, materiale fraudolento/illegale, gioco d'azzardo, materiale blasfemo o molesto/osceno.

g. Le informazioni relative ai siti acceduti (log files) possono essere utilizzate per analisi anche d'ordine statistico, dirette al perseguimento di finalità organizzative, produttive e di sicurezza. I dati raccolti vengono conservati per il tempo strettamente necessario alle suddette analisi e finalità.

8. Intranet e dominio istruzione.it

I servizi di posta elettronica del dominio istruzione.it, quelli forniti dal sito https://www.miur.gov.it e dalla intranet ministeriale sono direttamente gestiti dalla **Direzione Generale per i Sistemi Informativi** che ha diffuso specifiche informative in merito alle modalità di utilizzo dei suddetti servizi reperibili al seguente link https://www.miur.gov.it/dgsis

8.1 Utenti autorizzati all'uso di Internet

Per quanto riguarda l'uso delle dotazioni informatiche e l'accesso ad internet si individuano 4 tipologie di utenti:

1) **Personale tecnico**: autorizzato all'uso limitatamente allo svolgimento delle proprie mansioni o alle disposizioni ricevute
2) **Personale amministrativo**: autorizzato all'uso per lo svolgimento dell'attività amministrativa
3) **Personale docente**: autorizzato all'uso per qualunque attività educativa, didattica e formativa o ad esse anche indirettamente collegata.
4) **Alunni:** autorizzato limitatamente all'attività educativa, didattica e formativa programmata dai docenti

8.2 Ubicazione postazioni di lavoro

Per quanto riguarda il personale amministrativo, ogni dipendente riceve indicazione della postazione di lavoro a lui assegnata al momento della presa di servizio, ovvero in caso di cambiamento della propria posizione. L'uso di tale postazione non è tuttavia da ritenersi esclusivo e ciascun dipendente a seconda delle necessità potrà operare su altro PC non direttamente assegnato ***usando sempre la propria credenziale di accesso personale*** (nome utente e password).

L'accesso ad Internet da parte del personale tecnico, docente e degli alunni potrà avvenire nelle classi, nei laboratori ed in qualunque altro luogo a tale attività destinato.

8.3 Sistema di autenticazione

Al fine di ridurre al minimo il rischio di impieghi abusivi, l'accesso alle postazioni destinate all'attività amministrativa è protetto tramite sistema di autenticazione che richiede l'immissione di un apposito codice utente e della relativa password. La gestione degli utenti è fatta in maniera centralizzata sul server di segreteria su cui è configurato un dominio in ambiente Windows server e nel quale potranno quindi essere conservate informazioni relative agli accessi dei singoli utenti.

A causa degli eccessivi costi di gestione, non si è potuto fino ad ora realizzare un analogo sistema di autenticazione centralizzato per la gestione degli utenti relativi all'attività didattica (alunni, docenti e personale tecnico). Per questo motivo, non potendo garantire sulla rete destinata all'attività didattica le misure minime di sicurezza previste dall'allegato b del D.Lgs 196/03, non è autorizzato il trattamento di dati personali sui PC collegati alla rete didattica d'istituto.

8.4 Misure di tipo tecnologico connesse all'uso di Internet

L'Istituto intende limitare, per quanto possibile, i controlli sulla
navigazione che potrebbero determinare il trattamento di informazioni personali o sensibili anche non pertinenti l'amministrazione.

Per tale motivo è fondamentale il rispetto delle disposizioni elencate, che hanno il fine di ridurre il rischio di usi impropri della "navigazione".

1. Al personale non è consentito:
    - servirsi o dar modo ad altri di servirsi della stazione di accesso a internet per attività non istituzionali, per attività poste in essere in violazione del diritto d'autore o altri diritti tutelati dalla normativa vigente;
    - utilizzare sistemi Peer to Peer (P2P), di file sharing, podcasting, webcasting, social network o similari (salvo specifiche attività espressamente autorizzate per le finalità istituzionali).
2. Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico mediante virus o mediante ogni altro software aggressivo (attenzione nell'aprire mail e relativi allegati, non navigare su siti poco professionali, ecc..)
3. Ogni utente è tenuto a controllare la presenza e il regolare funzionamento del software antivirus, segnalando ogni eventuale problema all'amministratore di sistema.

Si ricorda poi che scaricare file audio e video (o comunque grandi quantità di dati) è in grado di degradare le prestazioni offerte dal servizio agli altri utenti: per tale motivo ciò può avvenire solo se necessario e, possibilmente, al di fuori dei momenti "di punta" a livello di Istituto.

Per garantire la sicurezza informatica ed il controllo del corretto utilizzo dell'accesso ad Internet l'istituto si è dotato di strumenti specifici che consentono:

- La protezione da accessi non autorizzati provenienti da Internet
- Controlli antivirus centralizzati
- configurazione di filtri che prevengono determinate operazioni non correlate all'attività lavorativa (quali a titolo esemplificativo e non esaustivo: l'accesso ai siti inseriti in black list individuati dall'Istituto, il download di file o software aventi particolari caratteristiche dimensionali o di tipologia di dato), anche in modo differenziato per le diverse postazioni o tipologie di accesso;
- la determinazione di informazioni sulla navigazione Internet che consentono la conservazione di informazioni relative ad utente, PC, ora di accesso, pagine accedute, etc.

Si precisa che ulteriori tracce dell'operato di ciascun utente, lasciate sui PC, sui server e sui programmi impiegati, potranno essere utilizzate per l'individuazione e la sanzione di eventuali comportamenti anomali.
La conservazione nel tempo dei dati relativi all'uso degli strumenti informatici verrà fatta per il periodo strettamente limitato al perseguimento di finalità organizzative, produttive e di sicurezza ovvero in adempimento di obblighi previsti dalla legge;

Art. 9: Utilizzo del servizio di Posta Elettronica dell'Istituto

a. La Posta Elettronica che l'Istituto mette a disposizione deve essere utilizzata in modo pertinente allo svolgimento dell'attività lavorativa, secondo un utilizzo appropriato, efficiente, corretto e razionale nel rispetto del principio di riservatezza.
I lavoratori assegnatari delle caselle di Posta Elettronica sono responsabili del corretto utilizzo delle stesse e vi debbono accedere a mediante autenticazione informatica ***user-id*** e ***password***.
b. I lavoratori sono tenuti, in un'ottica di correttezza ed uso responsabile degli strumenti, a contribuire alla riduzione del fenomeno dello "**spam**" (trasmissione su larga scala e in grandi volumi di e-mail non sollecitati): evitando di rispondere e/o inviare ad altri destinatari eventuali messaggi, del tipo "catene di Sant'Antonio", non sollecitati, che siano stati ricevuti, ed evitando di comunicare ad altri destinatari, in modo indiscriminato, il proprio indirizzo di posta elettronica o quello di colleghi.
c. I lavoratori non devono condurre attività commerciali di qualsiasi tipo a beneficio proprio e/o di terzi servendosi della Posta Elettronica dell' Istituto.
d. E' fatto divieto, in ogni caso, di trasmettere a chiunque ,a mezzo Posta Elettronica, materiale pornografico, materiale fraudolento/illegale, gioco d'azzardo, materiale blasfemo o molesto/osceno.
Il predetto divieto riguarda tanto il contenuto quanto gli allegati dei messaggi di Posta.
e. I lavoratori per adempiere il proprio dovere di diligenza e vigilanza nell'utilizzo dei beni e strumenti ad esso affidati hanno l'obbligo di impedire ad altri indebiti utilizzi della propria apparecchiatura informatica, non rilevando, al fine del difetto di responsabilità, il fatto che altri, in sua assenza, abbia potuto usare la postazione lavorativa. In difetto, il comportamento si configura come negligente, inescusabile e

gravemente colposo (p.to 1 ultimo paragrafo Direttiva 02/09 Dipartimento della funzione Pubblica).

f. Per evitare ogni interferenza con la sfera privata del personale docente e ATA, qualunque comunicazione di interesse amministrativo o di lavoro dovrà avvenire per mezzo delle caselle **istituzionali : rmic8fw00e@istruzione.it**

rmic8fw00e @pec.istruzione.it

La consultazione della posta elettronica da parte dei dipendenti può quindi riguardare:

- caselle personali: su dominio istruzione.it, messa a disposizione da parte del MIM (e/o casella personale privata, su altro dominio)
- caselle istituzionali di lavoro summenzionate

A. UTILIZZO DELLE CASELLE PERSONALI

Il personale può consultare in orario di servizio caselle personali per motivi legati alla propria attività lavorativa. La gestione deve essere effettuata tramite servizi di "webmail": non è consentito configurare su computer dell'Istituto appositi programmi tipo Outlook o Thunderbird per gestire le proprie caselle personali (anche per garantire al dipendente la dovuta riservatezza).

Nell'uso di caselle personali all'interno della scuola, al dipendente non è comunque consentito:

- inviare messaggi dannosi, di tipo offensivo o sconveniente, come ad esempio, a titolo non esaustivo, messaggi che riportino contenuti o commenti oltraggiosi su argomenti sessuali, razziali, religiosi, politici, ecc. e comunque ogni altra tipologia di messaggio che possa arrecare danno alla reputazione della Scuola o del MIM;
- l'uso del servizio di posta elettronica a scopi commerciali o di profitto personale e per attività illegali;
- utilizzare tecniche di "mail spamming" cioè di invio massiccio di comunicazioni a liste di distribuzione extra lavorative o azioni equivalenti.

B. UTILIZZO DELLE CASELLE ISTITUZIONALI DI LAVORO

Le caselle istituzionali sono gestite dagli incaricati in base ai compiti loro assegnati. In caso di assenza dell'incaricato abituale, questo potrà essere sostituito da altro personale, in base all'organizzazione interna del lavoro disposta dal Dirigente Scolastico o dal D.S.G.A.: quindi tali caselle devono essere utilizzate solo a scopo lavorativo e **NON devono essere utilizzate come caselle personali.**

Oltre alle disposizioni impartite per l'utilizzo delle caselle personali, si aggiungono le seguenti disposizioni:

- Evitare di aprire messaggi provenienti da mittenti sconosciuti e che contengono allegati sospetti (file con estensione .exe, .scr, .pif, .bat, .cmd,….). In caso di dubbio consultare un tecnico.
- Nel caso in cui si debba inviare un documento all'esterno dell'Istituto, se non specificamente destinato alla modifica, è preferibile utilizzare il formato *.pdf.
- Evitare che la diffusione incontrollata di "Catene di Sant'Antonio" (messaggi a diffusione capillare e moltiplicata) limiti l'efficienza del sistema di posta.
- Evitare di inviare allegati di dimensioni eccessive (se necessario usare formati compressi come *.zip, *.rar,…)
- L'iscrizione a "mailing list" esterne è concessa solo per motivi professionali, prima di iscriversi occorre verificare in anticipo se il sito è affidabile.
- La casella di posta deve essere mantenuta in ordine.

Art. 10: Priorità delle misure tecniche di protezione

1. L'Amministrazione si impegna ad attuare, in primo luogo, misure tecniche di protezione contro l'utilizzazione abusiva e i guasti tecnici ad esempio individuando categorie di siti correlati con l'attività lavorativa, creando una black list di siti proibiti, filtrando l'accesso a taluni siti in modo da impedire la navigazione in quelli non graditi. Tali misure sono regolarmente adeguate allo stato più recente della tecnica.
2. L'Amministrazione in nessun caso utilizza "programmi spia" o effettua controlli prolungati, costanti o indiscriminati.

Art. 11: Gradualità dei controlli

a. Qualsiasi forma di controllo viene effettuata, in quanto strettamente necessaria per il Datore di lavoro in relazione a scopi determinati e per il perseguimento di finalità organizzative, produttive e di sicurezza.

b. Nell'eventualità di anomalie riscontrate nell'utilizzo da parte dei lavoratori degli strumenti di lavoro messi a disposizione dall'Istituto, Il Dirigente Scolastico e l'Amministratore di Sistema, effettuano una prima segnalazione, nella quale non può essere indicato alcun nominativo di lavoratori, al D.S.G.A indicando il computer nel quale è stata rilevata l'anomalia. Quest'ultimo provvede, a sua volta, ad inviare un avviso generalizzato diretto a tutti i lavoratori appartenenti alla sua Struttura, nel quale evidenzia l'utilizzo irregolare degli strumenti dell'Istituto e invita i lavoratori medesimi ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.

c. Se l'avviso generalizzato di cui al comma **b.** non produce effetto e l'anomalia rilevata persiste, il Dirigente Scolastico e l'Amministratore di Sistema, procedono ad un controllo su base individuale e nominativa, a seguito del quale il medesimo Dirigente Scolastico effettua una seconda segnalazione al D.S.G.A. indicando l'area presso la quale è inserito il lavoratore interessato dalle verifiche.

Il Dirigente Scolastico, effettuate le necessarie verifiche, attiverà direttamente il procedimento disciplinare nei confronti del Lavoratore ai sensi dell'art. 55-bis c.2 del D.lgs. n. 165 del 30/03/2001 qualora il fatto sia di gravità tale da comportare una sanzione tra quelle di sua competenza.

L'Istituto è tenuta alla riservatezza in tutte le fasi di accertamento dei fatti

d. La rilevazione delle anomalie e delle verifiche tecniche di cui ai precedenti commi **b** e **c**, è a cura dell'Amministratore di Sistema. Responsabile dei successivi e consequenziali provvedimenti è il Dirigente Scolastico.

e. L'Istituto, nel rispetto del principio di protezione dei dati personali e del divieto di controllo a distanza del lavoratore, procede, in caso di anomalie, alla conservazione delle "registrazioni a giornale" (log file) relative all'utilizzazione di Internet , della Posta Elettronica e del telefono fisso nonché dei files con il dettaglio dei numeri chiamati totalmente "in chiaro" delle telefonate, dei Fax e dei Fax mail, per il tempo strettamente necessario alla soluzione delle suddette anomalie.

Art. 12: Obbligatorietà e Sanzioni

a. È fatto obbligo a tutti i Lavoratori di osservare le disposizioni del presente disciplinare e qualunque altra comunicata dall'Amministrazione in materia di sicurezza e gestione delle attrezzature informatiche.

b. Il mancato rispetto o la violazione delle regole contenute nel presente Disciplinare è perseguibile con tutte le azioni civili e penali previste dalla legge, nonché con i provvedimenti disciplinari, in conformità a quanto previsto dalle disposizioni normative e contrattuali vigenti per il personale o per l'area dirigenza.

Rimane ferma ogni ulteriore forma di responsabilità civile e penale in ordine a fattispecie quali.:

- violazione della privacy e della tutela dell'immagine;
- diffamazione;
- accesso abusivo ad un sistema informatico e telematico;
- violazione della legge sul copyright.

Art. 13: Gestione della casella di Posta Elettronica di un lavoratore cessato dal servizio

1. In caso di cessazione del rapporto di lavoro l'account di Posta Elettronica del lavoratore è prontamente bloccato e la sua casella di Posta Elettronica non è più funzionante.

2. I mittenti di email inviate all'indirizzo e-mail bloccato vengono automaticamente informati che l'indirizzo del destinatario è estinto al momento della cancellazione dell'account.

Art. 14: Esercizio dei diritti

1. I lavoratori possono esercitare i diritti previsti dal D.Lgs. 196/2003 s.m.i. rivolgendosi al Titolare del trattamento.

Art. 15: Disposizioni ulteriori

1. I dati personali inerenti i lavoratori non possono essere portati a conoscenza di terzi non autorizzati. I colleghi di lavoro della persona interessata sono considerati terzi.

2. L'Istituto, nell'ambito di procedimenti disciplinari e/o di procedimenti penali di cui all'art. 11 del presente Disciplinare e nel rispetto del principio di protezione dei dati personali e del divieto di controllo a distanza del lavoratore, procede alla conservazione delle "registrazioni a giornale" (log file) relative all'utilizzazione di Internet e/o della Posta Elettronica e/o dei files delle telefonate e/o dei Fax e dei Fax mail, fino alla conclusione dei relativi procedimenti.

3.Il presente documento viene portato a conoscenza di tutti i lavoratori, indicati all'art. 1 del presente Disciplinare, mediante pubblicazione nei sito internet.

16. Aggiornamento periodico

Il presente Disciplinare è aggiornato con cadenza almeno annuale o in caso di rinvenimento di soluzioni tecnologiche ritenute più idonee a tutelare i dati personali dei lavoratori, e portato a conoscenza di tutti i lavoratori mediante affissione all'albo dell'istituto e pubblicazione nell'intranet istituzionale.

ALLEGATO 3

REGOLAMENTO RELATIVO ALLA IDENTIFICAZIONE E ALLE MODALITÀ DI TRATTAMENTO DEI DATI SENSIBILI E GIUDIZIARI DEL PERSONALE SCOLASTICO E DEGLI ALUNNI

Si richiama qui espressamente quanto contenuto nel punto**1. Le Banche Dati dell'Istituto Scolastico** del Documento sulla Sicurezza e si identificano dettagliatamente **i dati sensibili e giudiziari trattati** e le relative operazioni effettuate dall'Istituto scolastico in riferimento agli interessati sotto indicati, in quanto di interesse concorrente e rilevante per il singolo e per la Istituzione Scolastica, alla luce di quanto disposto dall' art. 34 del D.Leg.vo 196/2003 s.m.i. e delle disposizioni contenute nel regolamento MIUR n°305/2006.

Dipendenti:

a. Documentazione riguardante il personale docente e non docente, 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.
b. Gestione del contenzioso e procedimenti disciplinari

Alunni:

a. Attività propedeutiche all'avvio dell'anno scolastico
b. Documenti riguardanti gli alunni, relativi al corso di studi, alla presenza di handicap, alla certificazione dell'idoneità alla pratica sportiva non agonistica, alla scelta dell'insegnamento della religione cattolica, all'esito di scrutini, esami, piani educativi individualizzati differenziati;
c. Documenti prodotti dalle famiglie riguardanti la certificazione della situazione patrimoniale e delle condizioni economiche.
d. Altri Rapporti scuola – famiglie
e. Organismi collegiali e commissioni istituzionali

A. DIPENDENTI

1. Documentazione riguardante il personale docente e non docente, 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

II trattamento dei Dati deve avere luogo soltanto in quanto necessario per l'attivazione delle 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 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 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.

I dati sono raccolti su iniziativa degli interessati o previa richiesta dell'Ufficio presso i medesimi interessati, ovvero presso altri soggetti pubblici o privati, e sono trattati, sia in forma cartacea che telematica, per l'applicazione dei vari istituti disciplinati dalla legge e dai regolamenti in materia di selezione, reclutamento, gestione giuridica, economica, previdenziale, pensionistica, aggiornamento e formazione del personale.

I dati potranno, altresì, essere comunicati a i Soggetti Pubblici sotto indicati per le seguenti finalità:

I. Servizi sanitari competenti per le visite fiscali e per l'accertamento dell'idoneità all'impiego;
II. Organi preposti al riconoscimento della causa di servzio/equo indennizzo, ai sensi del DPR 461/2001;
III. Organi preposti alla vigilanza in materia di igiene e sicurezza sui luoghi di lavoro (D.Lvo 81/2008 s.m.i .)
IV. 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 D.P.R. n. 1124/1965 ;
V. Amministrazioni provinciali per il personale assunto obbligatoriamente ai sensi della L. 68/1999;
VI. Organizzazioni sindacali per gli adempimenti connessi al versamento delle quote di iscrizione e per la gestione dei permessi sindacali;
VII. Pubbliche Amministrazioni presso le quali vengono comandati i dipendenti, o assegnati nell'ambito della mobilità;
VIII. Ordinario Diocesano per il rilascio dell'idoneità all'insegnamento della Religione Cattolica ai sensi della Legge 18 luglio 2003, n. 1 86;

IX. 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 D.P.R. 20 febbraio 1998, n.38;

X. Agenzia delle Entrate: ai fini degli obblighi fiscali del personale ex Legge 30 dicembre 1991, n. 413;

XI. MEF e INPS: per la corresponsione degli emolumenti connessi alla cessazione dal servizio ex Legge 8 agosto 1995, n. 335;

XII. Presidenza del Consiglio dei Ministri per la rilevazione annuale dei permessi per cariche sindacali s funzioni pubbliche elettive (art. 50, comma 3, d.lg. n. 165/2001).

2. Gestione del contenzioso e procedimenti disciplinari

II trattamento dei Dati deve avere luogo soltanto in quanto necessario per tutte le attività relative alla difesa in giudizio del Ministero dell'istruzione e delle istituzioni scolastiche ed educative nel contenzioso del lavoro e amministrativo nonché quelle connesse alla gestione degli affari penali e civili.

I dati potranno, altresì, essere comunicati a i Soggetti Pubblici sotto indicati per le finalità per le seguenti finalità:

I. 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 s.m.i.;

II. Organi arbitrali: per lo svolgimento delle procedure arbitrali ai sensi dei CCNL di settore; -

III. Avvocature dello Stato: per la difesa erariale e consulenza presso gli organi di giustizia;

IV. Magistrature ordinarie e amministrative-contabile e Organi di polizia giudiziaria: per l'esercizio dell'azione di giustizia;

B. *ALUNNI:*

1. Attività propedeutiche all'avvio dell'anno scolastico

I dati sono forniti dagli alunni e dalle famiglie ai fini della frequenza dei corsi di studio. II trattamento deve avere luogo soltanto in quanto necessario per tutte le attività propedeutiche all'avvio dell'anno scolastico da parte dell'Istituto Scolastico. Possono, quindi, essere trattati dati sensibili relativi:

- alle origini razziali ed etniche, per favorire l'integrazione degli alunni con cittadinanza non italiana;
- 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;
- allo stato di salute, per assicurare l'erogazione del sostegno agli alunni diversamente abili e per la composizione delle classi;
- 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 dell'alunno nonché nei confronti degli alunni che abbiano commesso reati.

I dati potranno, altresì, essere comunicati ai Soggetti Pubblici sotto indicati per le seguenti finalità:

I. agli Enti Locali per la fornitura dei seirvizi ai sensi del D. Lgsl. 31 marzo 1998, n. 112, limitatamente ai dati indispensabili all'erogazione del servizio;
II. ai gestori pubblici 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;
III. alle ASL e agli Enti Locali per il funzionamento dei Gruppi di Lavoro Handicap di istituto e per la predisposizione e verifica del Piano Educativo Individualizzato, ai sensi della Legge 5 febbraio 1992, n. 104;

2. Documenti riguardanti gli alunni, relativi al corso di studi, alla presenza di handicap, alla certificazione dell'idoneità alla pratica sportiva non agonistica, alla scelta dell'insegnamento della religione cattolica, all'esito di scrutini, esami, piani educativi individualizzati differenziati;

Dati sensibili possono essere trattati nell'espletamento delle attività educative, didattiche e formative, curriculari ed extracurriculari, di valutazione ed orientamento, di scrutini ed esami, relativamente:

I. alle origini razziali ed etniche per favorire l'integrazione degli alunni con cittadinanza non italiana;
II. alle convinzioni religiose per garantire la libertà di credo religioso;
III. allo stato di salute, per assicurare l'erogazione del servizio di refezione scolastica, del sostegno agli alunni disabili, dell'insegnamento domiciliare ed ospedaliere 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;
IV. ai dati giudiziari, per assicurare il diritto allo studio anche a soggetti sottoposti a regime di detenzione;
V. alle convinzioni politiche, per la costituzione e il funzionamento delle Consulte e delle Associazioni degli studenti e dei genitori

I dati sensibili possono, altresì, essere trattati per le attività di valutazione periodica e finale, per le attività di orientamento e per la compilazione della certificazione delle competenze. I dati potranno essere comunicati ai Soggetti Pubblici sotto indicati per le seguenti finalità :

I. Alle altre istituzioni scolastiche, statali e non statali, per la trasmissione della documentazione attinente la carriera scolastica degli alunni, limitatamente ai dati indispensabili all'erogazione del servizio;
II. agli Enti Locali per la fornitura dei servizi ai sensi del D. Lgsl. 31 marzo 1998, n. 112, limitatamente ai dati indispensabili all'erogazione del servizio;
III. ai gestori pubblici 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 ali1 erogazione del servizio;
IV. agli Istituti di assicurazione per denuncia di infortuni e per la connessa responsabilità civile;
V. all'INAIL per la denuncia di infortuni ex-D.P.R. 30 giugno 1965, n. 1124 s.m.i.;

VI. alle AUSL e agli Enti Locali per il funzionamento dei Gruppi di Lavoro di istituto per l'Handicap e per la predisposizione e la verifica del Piano Educativo Individuale, ai sensi della Legge 5 febbraio 1992, il 104;

VII. ad aziende, imprese e altri soggetti pubblici o privati per tirocini formativi, stages e alternanza scuola-lavoro, ai sensi della Legge 24 giugno 1997, n. 196 e del D. Lgsl. 21 aprile 2005, n. 77 e, facoltativamente, per attività di rilevante interesse sociale ed economico, limitatamente ai dati indispensabili all'erogazione del servizio.

3.Rapporti scuola – famiglie: gestione del contenzioso

II trattamento di dati sensibili e giudiziari concerne tutte le attività connesse alla instaurazione di contenzioso (reclami, ricorsi, esposti, provvedimenti di tipo disciplinare, ispezioni, citazioni, denunce all'autorità giudiziaria, etc.) con gli alunni e con le famiglie, e tutte le attività relative alla difesa in giudizio dell'Istituto Scolastico.

I dati potranno essere comunicati ai Soggetti Pubblici sotto indicati per le seguenti finalità :

I. Avvocatura dello Stato, per la difesa erariale e consulenza presso gli organi di giustizia;

II. Magistrature ordinarie e amministrative-contabile e Organi di polizia giudiziaria, per l'esercizio dell'azione di giustizia;

III. Liberi professionisti, ai fini di patrocinio o di consulenza, compresi quelli di controparte per le finalità di corrispondenza.

4. Organismi collegiali e Commissioni istituzionali

Dati sensibili possono essere trattati soltanto se è necessario per attivare gli organismi collegiali e le commissioni istituzionali previsti dalle norme di organizzazione del Ministero Istruzione e dell'ordinamento scolastico. Tali organi sono rappresentativi sia del personale amministrativo e scolastico, sia degli studenti, delle famiglie e delle associazioni sindacali.

Il dato sensibile trattato è quello dell'appartenenza alle organizzazioni sindacali, con riferimento agli organismi o comitati che richiedano la partecipazione di rappresentati delle organizzazioni sindacali.

ALLEGATO 2a.

INFORMATIVA EX ART. 13 D.LGS. N. 196/2003 s.m.i. PER IL TRATTAMENTO DEI DATI DEL PERSONALE DIPENDENTE

Egr……..

Questo Istituto Scolastico presso cui Ella presta servizio, potrebbe avere la necessità di trattare i suoi dati personali. Pertanto, qualora se ne ravvisi la necessità, il trattamento dei dati personali che La riguardano sarà effettuato secondo i principi di correttezza, liceità e trasparenza e di tutela della Sua riservatezza e dei Suoi diritti così come previsto dal D.lgs. n. 196/2003 s.m.i. ("Codice in materia di protezione dei dati personali ") che prevede, appunto, la tutela delle persone fisiche e giuridiche in relazione al trattamento dei relativi dati personali.

Ai sensi dell'art. 13 del D.lgs. n.196/2003, pertanto, La informo che:

Il Titolare del Trattamento dei Dati è l'Istituto Comprensivo Nelson Mandela codice fiscale 97712890587 Tel. 0666000349 E-mail rmic8fw00e@pec.istruzione.it nella persona del Dirigente Scolastico pro tempore **Prof.ssa Maria Canosa.**

Il Responsabile del Trattamento dei Dati è la **D.S.G.A. Sig. Nicolina Piluso**
Tel. 0666000349 E-mail rmic8fw00e@pec.istruzione.it

A. I dati personali da Lei forniti verranno trattati esclusivamente per le finalità istituzionali della scuola, che sono quelle della istruzione e formazione degli alunni nonché quelle amministrative ad esse strumentali, incluse le finalità di instaurazione e gestione dei rapporti di lavoro.
B. I dati potranno essere trattati anche con strumenti elettronici ed informatici e saranno memorizzati su supporti informatici, su supporti cartacei e su ogni altro tipo di supporto idoneo, nel rispetto del Disciplinare Tecnico in materia di misure minime di sicurezza, Allegato B del D.lgs. n.196/2003.
C. Il conferimento dei dati che Le vengono richiesti è obbligatorio ed è

esplicitamente consentito dalla normativa richiamata: l'eventuale rifiuto di fornire tali dati comporta il mancato perfezionamento o mantenimento del rapporto di lavoro;

E. Il trattamento potrà avere ad oggetto anche dati "sensibili" e "giudiziari", così come definiti dal D. L.vo 196/2003, secondo le modalità previste dal Decreto del Ministero della Pubblica Istruzione n. 305 del 7 dicembre 2006 che ha individuato i dati sensibili e giudiziari che le amministrazioni scolastiche sono autorizzate a trattare, indicando anche le operazioni ordinarie che i diversi titolari devono necessariamente svolgere per perseguire le finalità di rilevante interesse pubblico individuate per legge. L'Istituto mette a disposizione per la consultazione il regolamento per il trattamento di dati sensibili e giudiziari nelle amministrazioni scolastiche emanato dal Ministero della Pubblica Istruzione.
Potranno venire a conoscenza dei Suoi dati personali, in qualità di responsabili o incaricati: il dirigente scolastico, il direttore dei servizi amministrativi, il personale addetto ai servizi amministrativi, i docenti.

F. Ella ha facoltà di rivolgersi al o al responsabile titolare del trattamento dei dati, per far valere i Suoi diritti, così come previsto dall'articolo 7 del D.lgs.196/2003 [1].

[1] **Art. 7 del Decreto Legislativo n.196/2003 (Diritto di accesso ai dati personali ed altri diritti)**
1. L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile.
2. L'interessato ha diritto di ottenere l'indicazione:
a) dell'origine dei dati personali;
b) delle finalità e modalità del trattamento;
c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sens i dell'articolo 5, comma 2;
e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.
3. L'interessato ha diritto di ottenere:
a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati;
la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi

ALLEGATO 2b .

ACQUISIZIONE DEL CONSENSO DEL SOGGETTO INTERESSATO AL TRATTAMENTO DEI DATI AI SENSI DEL D.L.VO 196/2003 s.m.i.

Si informa che per poter svolgere l'attività ***(indicare il tipo di attività)***: gita, visita di istruzione, ECDL) pertinente alle attività istituzionali e connessa ad attività strumentali alle stesse, si rende necessario comunicare alcuni dati personali dello studente……, in possesso dell'Istituto Scolastico a……(*indicare a quale soggetto non* istituzionale saranno comunicati i dati ….)
Tali dati, diversi da quelli sensibili e giudiziari, e più precisamente(nome, cognome, luogo e data di nascita, indirizzo, ….) verranno trattati esclusivamente per la suddetta attività e non saranno comunicati ad altri soggetti, né saranno oggetto di diffusione.
Secondo le norme contenute nel D. L.vo 196/2003 s.m.i., tale trattamento sarà improntato ai principi di necessità, liceità, correttezza, finalità, proporzionalità, qualità dei dati (esatti, aggiornati, pertinenti, completi e non eccedenti) e alla tutela della sua riservatezza e dei diritti dell'interessato.
L'eventuale rifiuto a prestare il consenso potrebbe comportare l'impossibilità di usufruire dell'attività come programmata.

Data……

Il Dirigente Scolastico

……

I sottoscritti……esercenti la genitoria potestà sul minore…… nome e cognome dell'alunno
acquisite le informazioni fornite dal titolare del trattamento ai sensi dell'art. 13 del D.L.vo 196/03, prestano il loro consenso al trattamento dei dati personali per i fini su indicati
Per accettazione

(firma)
……

ALLEGATO 2c

MODULO PER LA RICHIESTA DI ACCESSO AL TRATTAMENTO

Il sottoscritto ……, nato a …… il …… , residente in …… ai sensi dell'art. 7 del Testo Unico in materia di trattamento di dati personali di cui al D. L.vo n. 196/2003 s.m.i.

chiede

di essere informato sull'identità dei responsabili e sulle finalità e modalità del trattamento svolto da codesto Istituto Scolastico

chiede inoltre di ottenere *(barrare la casella che interessa***)**

- o la conferma dell'esistenza o meno di dati che lo riguardano
- o la cancellazione dei dati perché trattati in violazione dell'art…….
- o la trasformazione in forma anonima perché in violazione legge…..
- o il blocco dei dati per violazione delle disposizioni……
- o l'aggiornamento……
- o la rettificazione……
- o l'integrazione……
- o Dichiara di opporsi al trattamento dei dati che lo riguardano per i seguenti motivi……

_____ Firma Interessato

PARTE SPECIALE TERZA

NOMINE ED INCARICHI

1. **Determina Dirigenziale di nomina del Responsabile del Trattamento dei dati;**
2. **Nomina dell'Amministratore del Sistema Informatico;**
3. **Nomina dell'Incaricato delle copie di sicurezza;**
4. **Nomina dell'Incaricato dei dati personali (Assistente Amministrativo;)**
5. **Disposizioni per l'Assistente Amministrativo incaricato del trattamento;**
6. **Nomina dell'Incaricato del trattamento dei dati personali (Assistente Tecnico);**
7. **Nomina dell'Incaricato del trattamento dei dati personali (Collaboratore Scolastico)**
8. **Disposizioni per il Collaboratore Scolastico incaricato del trattamento**
9. **Nomina dell'Incaricato del trattamento dei dati personali (Docenti);**
10. **Disposizioni per i Docenti incaricati del trattamento;**
11. **Elenco degli incaricati del trattamento dei dati che utilizzano dotazioni informatiche.**

1. DETERMINA DIRIGENZIALE DI NOMINA DEL RESPONSABILE DEL TRATTAMENTO DEI DATI

(ART. 29 D.LGS.196/2003 s.m.i.)

Il Dirigente Scolastico Prof. .....Titolare del Trattamento dei Dati Personali gestiti dall'Istituto Scolastico……per finalità proprie, ai sensi dell'art. 29 del D.Lgs.196/2003,

PREMESSO CHE

- Il D.Lgs.196/2003 s.m.i. ha espressamente previsto la possibilità che il Titolare preponga al trattamento dei dati personali uno o più Responsabili del Trattamento dei Dati, scelti tra soggetti che, per la loro capacità, esperienza e affidabilità, forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di tutela dei dati personali, ivi compresa la sicurezza degli stessi;
- Il Responsabile deve procedere al trattamento con la dovuta diligenza, nonché attenendosi alle istruzioni ricevute dal Titolare, il quale deve vigilare sulla puntuale osservanza delle disposizioni vigenti;
- Il Titolare del trattamento dei Dati intende procedere alla nomina di **Responsabile del trattamento dei dati personali .....**, nella qualità di **DIRETTORE DEI SERVIZI GENERALI E AMMINISTRATIVI** per le seguenti banche dati:

  - Contabilità pubblica e patrimonio
  - dipendenti
  - protocollo
  - alunni
  - fornitori
  - rapporto con enti ed imprese

- il Responsabile del trattamento dei dati, previo avviso tempestivo e preventivo al Titolare del trattamento, è autorizzato ad affidare, sotto la sua responsabilità l'esecuzione di operazioni di trattamento soggetti che per esperienza, capacità ed affidabilità, forniscano anche idonea garanzia del pieno rispetto della legge, con particolare riguardo alla sicurezza. Questi soggetti si qualificano come **Incaricati del trattamento dei Dati.** del.....

Tanto premesso

NOMINA

RESPONSABILE DEL TRATTAMENTO DEI DATI (indicare la persona)
nella qualità di **DIRETTORE DEI SERVIZI GENERALI E AMMINISTRATIVI** affidando i compiti e le responsabilità previste dall'art. 29 del D.Lgs.196/2003 s.m.i. per le banche dati sopra indicate.

Con la sottoscrizione del presente atto…….accetta la nomina e s' impegna a procedere al trattamento dei dati di cui è Responsabile, attenendosi alle disposizioni seguenti:

A. Il **Responsabile del trattamento dei dati personali** ha il compito di curare lo svolgimento del trattamento dei dati attenendosi ai principi previsti dal D.Lgvo196/2003s.m.i. e a quanto previsto nel **Documento sulla Sicurezza Informatico** dell'Istituto Scolastico e provvede a:

- verificare la liceità e la correttezza dei trattamenti ai sensi dell'art.11 del D.Lgs. n.196/2003 mediante l'effettuazione di controlli periodici;
- valutare ed adottare per i trattamenti di propria competenza, anche con la collaborazione dell'Amministratore di Sistema, le misure di sicurezza idonee e preventive da adottare ai sensi degli articoli da 33 a 36 del D.Lgs. n.196/2003 s.m.i. e del disciplinare tecnico di cui all'allegato B, e ciò al fine di custodire e controllare i dati, in modo da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
- fornire le informative agli interessati, ai sensi dell'art. 13 del D.Lgs. n 196/2003 s.m.i.;
- raccogliere e conservare i moduli con il consenso espresso dagli interessati relativamente al trattamento dei dati sensibili;
- rispondere all'interessato, che eserciti i diritti ex art. 7 del D.Lgs. n.196/2003 s.m.i.;
- verificare la corrispondenza delle finalità del trattamento rispetto alle disposizioni di legge e soprattutto al consenso manifestato dall'interessato nel caso di trattamento di dati sensibili;

- dare istruzione all'Amministratore di Sistema per la revoca di tutte le credenziali non utilizzate in caso di perdita della qualità che consentiva all'incaricato l'accesso ai dati personali;
- dare istruzione all'Amministratore del Sistema Informatico per la revoca delle credenziali per l'accesso ai dati degli incaricati al trattamento nel caso di mancato utilizzo per oltre 6 mesi;
- individuare, nominare ed incaricare per iscritto gli **Incaricati del trattamento dei dati personali;**
- individuare, nominare ed incaricare per iscritto uno o più **Incaricati delle copie di sicurezza delle banche dati;**
- gestire e custodire le credenziali per l'accesso ai dati degli **Incaricati del trattamento;**
- Predisporre, per ogni **Incaricato del trattamento**, una busta sulla quale è indicato il nome dell'incaricato e all'interno della busta deve essere indicata la credenziale usata. Le buste con le credenziali debbono essere conservate in luogo chiuso e protetto;
- dare istruzioni adeguate alle figure da esso nominate

B. il **Responsabile del trattamento dei dati** può individuare, nominare ed incaricare per iscritto uno o più **Incaricati delle copie di sicurezza** cui sono affidate le seguenti funzioni e responsabilità:

- sovrintendere alla esecuzione periodica delle copie di sicurezza delle banche dati ad essi assegnati secondo le procedure definite dal **Responsabile del trattamento** o **dall'Amministratore di sistema ;**
- attenersi alle disposizioni ricevute dal **Responsabile del trattamento** in merito alla conservazione delle copie delle banche dati;
- conservare e custodire con la massima cura i dispositivi utilizzati per le copie di sicurezza, impedendo l'accesso agli stessi dispositivi da parte di personale non autorizzato;
- segnalare tempestivamente al Responsabile del trattamento dei Dati ogni eventuale problema dovesse verificarsi nella normale attività di copia

delle banche dati.

Qualora il **Responsabile del trattamento dei dati personali** ritenga di non nominare **Incaricati delle copie di sicurezza delle banche dati**, ne assumerà tutte le responsabilità e funzioni.

IL DIRIGENTE SCOLASTICO

(Titolare del trattamento) Prof.……

IL RESPONSABILE DEL TRATTAMENTO

D.S.G.A. ……(per accettazione)

2. NOMINA DELL'AMMINISTRATORE DEL SISTEMA INFORMATICO

Prot. n. ……
(Luogo)…….(Data)..

Il Dirigente Scolastico ……, in qualità di rappresentante legale dell'Istituto ……, Titolare del trattamento dei dati ai sensi del D.lgs N. 196 del 30/06/2003 s. m.i. ,

- ritenuto la necessità di individuare un soggetto al quale possa essere conferito il compito di sovrintendere alle risorse del sistema operativo degli elaboratorie del sistema delle varie banche dati dell'Istituto ….e di consentirne l'utilizzazione;
- ritenuto che lo stesso Garante per la protezione dei dati personali impone ai Titolari di trattamenti di dati personali di nominare amministratori di sistema dopo averne valutato l'esperienza, la capacità e l'affidabilità in modo da fornire idonea garanzia del pieno rispetto delle disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza;
- considerato che l'incarico attiene a fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati;
- constatata l'impossibilità di ricorrere a competenze interne;
- verificate le competenze della persona a cui è assegnato il presente incarico

NOMINA

il Sig……, in qualità di…….della Ditta……, Amministratore di sistema con i seguenti compiti:

- sovrintendere al funzionamento della rete, comprese le apparecchiature di protezione (firewall, filtri per la posta elettronica, antivirus, backup , disaster recovery, ecc);
- monitorare lo stato dei sistemi, con particolare attenzione alla sicurezza informatica;
- effettuare interventi di manutenzione hardware e software su sistemi operativi e applicativi;
- gestire, in collaborazione con il Responsabile del trattamento dei dati personali il sistema di attribuzione e gestione dei codici di accesso agli strumenti informatici;
- gestire le password di Amministratore di sistema;
- collaborare con il custode delle password;

- informare il Responsabile del trattamento o il Titolare in caso di mancato rispetto delle norme di sicurezza e in caso di eventuali incidenti.

L'Amministratore incaricato dichiara di essere a conoscenza e di rispettare quanto stabilito dal D.lgs n. 196 del 30/06/2003 s.m.i. ed in particolare:

1. di conoscere e impegnarsi a rispettare, sotto la propria responsabilità e nell'ambito delle materie oggetto del presente incarico, quanto indicato nell'allegato B del "Disciplinare tecnico in materia di misure minime di sicurezza";
2. di attenersi agli obblighi di assoluta riservatezza connessi al suo incarico;
3. di trattare dati personali solo se risulti indispensabile in relazione all'assolvimento degli incarichi assegnati;
4. di rispettare le prescrizioni impartite dal Titolare, tra cui il divieto assoluto di comunicare e diffondere a terzi non autorizzati le informazioni e i dati personali di cui sia venuto a conoscenza.

In questo quadro, s'impegna ad adottare tutte le misure necessarie all'attuazione di quanto descritto nel Documento sulla Sicurezza Informatica adottato dalla Istituzione scolastica, in relazione ai compiti sopra indicati.

Per accettazione dell'incarico	Il Titolare del trattamento
(NOME COGNOME)	(NOME COGNOME del Dirigente)

3. NOMINA DELL'INCARICATO DELLE COPIE DI SICUREZZA

(artt. 30,31 del D.Lvo 196/2003 s.m.i.)

…… Direttore dei Servizi generali e amministrativi (DSGA) di questo Istituto nella qualità **di Responsabile del trattamento dei dati**

Visto la Determina Dirigenziale emessa il con cui viene nominato Responsabile del Trattamento dei Dati;
Visti gli artt. 30,31 del D.Lvo 196/2003 s.m.i.;

nomina**……Incaricato delle copie di sicurezza.**
Agli **Incaricati delle copie di sicurezza** sono affidate le seguenti funzioni e responsabilità:

- sovrintendere alla esecuzione periodica delle copie di sicurezza delle banche dati ad essi assegnati secondo le procedure definite dal **Amministratore del sistema informatico;**
- attenersi alle disposizioni ricevute dal **Responsabile del trattamento dei Dati** in merito alla conservazione delle copie delle banche dati;
- conservare e custodire con la massima cura i dispositivi utilizzati per le copie di sicurezza, impedendo l'accesso agli stessi dispositivi da parte di personale non autorizzato;
- segnalare tempestivamente al **Responsabile del trattamento dei Dati** ogni eventuale problema dovesse verificarsi nella normale attività di copia delle banche dati.

In Roma il……

IL DIRETTORE DEI SERVIZI GENERALI ED AMMINISTRATIVI

(Responsabile del trattamento)

……

l'incaricato delle copie di sicurezza

…… (per accettazione)

4. NOMINA DELL'INCARICATO DEI DATI PERSONALI (ASSISTENTE AMMINISTRATIVO)
(artt. 30,31 del d.lvo 196/2003 s.m.i.)

IL DIRETTORE DEI SERVIZI GENERALI ED AMMINISTRATIVI
in qualità di Responsabile del trattamento dei dati personali dell'Istituto;

richiamate le norme di cui gli art. 29 e 30 del D. L.vo 196/03 s. m.i e considerato :

- che i sottoelencati Assistenti Amministrativi, nell'ambito delle loro mansioni compiono attività che possono comprendere il trattamento dei dati personali;
- che la nomina a Incaricato non implica l'attribuzione di funzioni ulteriori rispetto a quelle già assegnate al dipendente bensì costituisce un'autorizzazione a trattare dati personali e fornisce istruzioni sulle modalità cui attenersi nel trattamento;
- che pur permanendo obblighi e responsabilità civili e penali dei dipendenti pubblici nell'ambito delle attività d'ufficio, si dispone, sotto vincolo disciplinare, l'obbligo tassativo di attenersi alle istruzioni allegate da osservarsi dagli Assistenti Amministrativi qualora trattino dati personali;

NOMINA

1. **.....**
2. **.....**
3. **.....**
4. **.....**

INCARICATI DEL TRATTAMENTO DEI DATI PERSONALI

L'incaricato del trattamento dei dati **SI IMPEGNA**:

- a procedere al trattamento dei dati personali nel rispetto dei principi generali di cui all'art. 30 Del D.Lgs. n.196/2003 s.m.i.: in particolare i dati devono essere trattati in modo lecito e secondo correttezza;
- a raccogliere e registrare i dati per scopi determinati, espliciti e legittimi tenendo conto che devono essere pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;
- a rispettare i divieti di comunicazione e diffusione dei dati trattati nel corso del presente incarico e a non utilizzare i dati, cui abbia accesso, per finalità incompatibili con quelle relative al profilo di appartenenza. Si ricorda che le operazioni di comunicazione e diffusione di dati sensibili sono possibili quando vi sia una apposita previsione di legge o di regolamento;
- ad attenersi, nel loro operato, alle istruzioni per lo svolgimento delle operazioni di trattamento allegate alla presente determina.

La presente nomina è a tempo indeterminato e può essere revocata in qualsiasi momento dal Responsabile del trattamento dei dati personali senza preavviso. Peraltro si intende automaticamente revocata alla data di cessazione del rapporto di lavoro con questa istituzione scolastica, per trasferimento ad altra istituzione o cessazione del rapporto di lavoro.

E' fatto divieto di comunicazione e diffusione dei dati trattati nel corso dei presente incarico, anche per il tempo successivo alla sua cessazione, senza limiti temporali.

Qualunque violazione delle modalità sopra indicate e delle linee guida consegnate con la presente dà luogo a precise responsabilità ai sensi delle norme contenute nel D L.vo 196/03.

In Roma così dato il……

IL DIRETTORE DEI SERVIZI GENERALI ED AMMINISTRATIVI

(Responsabile del trattamento)

----

per presa visione e accettazione l'Incaricato del trattamento dei dati

…….

5. DISPOSIZIONI PER L'ASSISTENTE AMMINISTRATIVO INCARICATO DEL TRATTAMENTO

Il Responsabile del trattamento dei dati

Visti gli artt. 29 e 30 del D. L.vo 196/03 s. m.i;

richiamate le modalità del trattamento dei dati e sulle misure di sicurezza e contenute nel presente Documento Programmatico sulla Sicurezza,

EMETTE

le istruzioni cui dovrà attenersi scrupolosamente il personale amministrativo incaricato del trattamento dei dati personali e sensibili.

A. ***Riguardo ai trattamenti eseguiti con supporto cartaceo:***

I. Controllare e custodire gli atti e i documenti contenenti dati personali in modo da assicurarne l'integrità e la riservatezza;
II. Conservare sempre i dati del cui trattamento si è incaricati in apposito armadio assegnato;
III. Accertarsi della corretta funzionalità dei meccanismi di chiusura degli armadi, segnalando tempestivamente al Responsabile eventuali anomalie;
IV. fornire sempre l'informativa all'interessato o alla persona presso cui si raccolgono i dati prima di procedere alla raccolta e al trattamento dei dati;
V. consegnare, quando necessario, il modulo per il consenso da parte dell'interessato. Ricevere quindi il modello opportunamente firmato da parte dell'interessato o di chi lo rappresenti;
VI. limitare l'accesso ai dati personali, oggetto di trattamento, la cui conoscenza sia strettamente necessaria per lo svolgimento delle funzioni e dei compiti affidati e per le finalità di cui al provvedimento di incarico;
VII. conservare i documenti o atti che contengono dati sensibili o giudiziari in archivi (ad esempio stanze, armadi, schedari, contenitori in genere) chiusi a chiave;
VIII. Non fornire telefonicamente o a mezzo fax dati e informazioni relativi a terzi, senza una specifica autorizzazione del Responsabile;

IX. richiedere l'identità del chiamante e quindi provvedere a richiamare, avendo così la certezza sull'identità del richiedente, qualora giungano richieste telefoniche di dati sensibili da parte dell'Autorità Giudiziaria o degli organi di polizia;

X. Non fornire telefonicamente o a mezzo fax dati e informazioni ai diretti interessati senza avere la certezza della sua identità;

XI. Non inviare per fax documenti in chiaro contenenti dati sensibili;

XII. distruggere o comunque rendere illeggibili, prima di essere eliminati o cestinati i documenti cartacei non più utilizzati, specie se sensibili;

XIII. Vietare l'accesso a estranei e a soggetti non autorizzati alle aree in cui sono conservati dati personali su supporto cartaceo;

XIV. Conservare i documenti ricevuti da genitori/studenti o dal personale in apposite cartelline non trasparenti;

XV. Consegnare al personale o ai genitori/studenti documentazione inserita in buste non trasparenti;

XVI. Vietare l'accesso a estranei al fax e alla stampante che contengano documenti non ancora ritirati dal personale;

XVII. Effettuare esclusivamente copie fotostatiche di documenti per i quali si è autorizzati;

XVIII. Non lasciare a disposizione di estranei fotocopie inutilizzate o incomplete di documenti che contengono dati personali o sensibili ma accertarsi che vengano sempre distrutte;

XIX. Non lasciare incustodito, se esistente, il registro contenente gli indirizzi e i recapiti telefonici del personale e degli studenti e non annotarne il contenuto sui fogli di lavoro;

XX. Non lasciare la postazione di lavoro per la pausa o altro motivo senza aver provveduto a custodire in luogo sicuro i documenti trattati;

XXI. Segnalare tempestivamente al Responsabile la presenza dì documenti incustoditi provvedendo temporaneamente alla loro custodia;

XXII. Attenersi alle direttive ricevute e non effettuare operazioni per le quali non si è stati espressamente autorizzati dal Responsabile o dal Titolare.

B. ***Riguardo ai trattamenti eseguiti con supporto informatico:***

I. utilizzare le parole chiave definite dal Responsabile della gestione e della manutenzione del sistema informatico e alle quali sono associati le relative autorizzazioni per l'accesso al sistema informatico;
II. adottare le necessarie cautele per assicurare la segretezza della parola chiave e la diligente custodia di ogni altro dispositivo di autenticazione informatica (badge, schede magnetiche, chiavi USB, etc.)
III. E' fatto divieto comunicare a qualunque altro incaricato le proprie credenziali di accesso al sistema informatico;
IV. modificare almeno ogni sei mesi (tre mesi nel caso di dati sensibili) la parola chiave, che viene assegnata dal Responsabile del trattamento o dal Responsabile della gestione e della manutenzione del sistema informatico;
V. la parola chiave da consegnare all'Incaricato della custodia delle copie delle credenziali, che ne curerà la conservazione, deve essere chiusa in una busta opaca, sigillata e controfirmata sui lembi;
VI. Prevedere che soltanto il Responsabile o l'Incaricato della custodia delle copie delle credenziali abbiano la possibilità, previa comunicazione all'incaricato, di aprire la busta, per esigenze operative o di organizzazione. L'incaricato nel tal caso provvederà a sostituire la parola chiave violata;
VII. Provvedere a porre i pc e/o i terminali in condizione di non essere utilizzati da terzi estranei tutte le volte che si lascia incustodita la propria postazione di lavoro. In particolare si chiudano tutte le applicazioni in uso e si ponga un blocco del sistema mediante password;
VIII. spegnere sempre il PC alla fine della giornata lavorativa o in caso di assenze prolungate dalla postazione di lavoro;
IX. dare immediata comunicazione al Responsabile del Trattamento ; su difformità dei dati trattati o del funzionamento degli elaboratori
X. riutilizzare i supporti informatici, già utilizzati per il trattamento dei dati sensibili e giudiziari, solo se le informazioni precedentemente contenute non sono più in alcun modo recuperabili, dovendo altrimenti essere distrutti;
XI. Utilizzare l'antivirus per la verifica di ogni documento trattato o di qualunque file scaricato da Internet;
XII. Utilizzare sempre l'antivirus per verificare il contenuto di qualunque supporto di memorizzazione sospetto;

XIII. Aggiornare con frequenza l'antivirus e comunicare al Responsabile del trattamento dei dati ogni problema a riguardo;

XIV. informare il Responsabile del trattamento se l'antivirus riscontra la presenza di un virus informatico;

XV. Non installare sui PC alcun software senza l'autorizzazione del Responsabile del trattamento.

XVI. - E' vietato modificare le impostazioni effettuate sul sistema dal Responsabile della gestione e della manutenzione del sistema informatico

C. ***Regole per la scelta delle parole chiave***

I. usare una parola chiave di almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, costituita da un numero di caratteri pari al massimo consentito;

II. la parola chiave non deve contenere riferimenti facilmente riconducibili all'incaricato (come per esempio nome, cognome, data di nascita, numeri di telefono, etc. propri o dei propri familiari);

III. usare una combinazione di caratteri alfabetici e numerici, meglio se contenente almeno un segno di interpunzione o un carattere speciale;

IV. conservare con cura la parola chiave evitando di trascriverla su fogli posti in vista in prossimità del PC o sulla rubrica dell'ufficio.

IL DIRETTORE DEI SERVIZI GENERALI ED AMMINISTRATIVI

(Responsabile del trattamento)

6. NOMINA DELL'INCARICATO DEL TRATTAMENTO DEI DATI PERSONALI (ASSISTENTE TECNICO)

IL DIRETTORE DEI SERVIZI GENERALI ED AMMINISTRATIVI

in qualità di Responsabile del trattamento dei dati personali dell'Istituto;

tenuto conto del ruolo funzionale svolto da…….. nell' Istituto" istituzione scolastica;

considerato che, nell'ambito di tali mansioni il Sig.……compie attività che possono comprendere il trattamento dei dati personali;

richiamate le norme di cui gli art. 29 e 30 del Codice in materia di protezione dei dati personali D. L.vo 196/03 s. m.i.;

NOMINA ……INCARICATO DEL TRATTAMENTO DEI DATI PERSONALI

L'incaricato del trattamento dei dati **SI IMPEGNA**:

- a procedere al trattamento dei dati personali nel rispetto dei principi generali di cui all'art. 30 Del D.Lgs. n.196/2003 s.m.i.:
    1. raccolti e registrati per scopi determinati, espliciti e legittimi;
    2. i dati devono essere pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;
- a rispettare i divieti di comunicazione e diffusione dei dati trattati nel corso del presente incarico e a non utilizzare i dati, cui abbia accesso, per finalità incompatibili con quelle relative al profilo di appartenenza. Si ricorda che le operazioni di comunicazione e diffusione di dati sensibili sono possibili quando vi sia una apposita previsione di legge o di regolamento.
- ad attenersi, nel suo operato, alle istruzioni ricevute per lo svolgimento delle operazioni di trattamento.

Il Sig……. è inoltre autorizzato ad intervenire sui PC dell'Amministrazione per garantire un servizio di assistenza e manutenzione ordinaria del sistema informatico dell'Istituto, ivi compresi i PC della segreteria in cui avviene il trattamento di dati personali. Nello svolgimento di tale attività la S.V. dovrà: evitare qualunque accesso ai dati personali presenti nei PC a meno che questo non sia tecnicamente necessario allo svolgimento del compito ricevuto

- provvedere all'effettuazione preventiva della copia di sicurezza dei dati ogni qualvolta l'intervento tecnico comporti il rischio della perdita dei dati

- garantire la riservatezza e l'integrità dei dati personali trattati nello svolgimento dell'attività di assistenza tecnica e manutenzione

- rispettare i divieti di comunicazione e diffusione dei dati trattati nel corso del presente incarico e a non utilizzare i dati, cui abbia accesso, per finalità incompatibili con quelle relative al profilo di appartenenza.

La presente nomina di Incaricato ai trattamento dei dati personali è a tempo indeterminato e può essere revocata in qualsiasi momento dal Responsabile del trattamento dei dati personali senza preavviso. La presente nomina si intende automaticamente revocata alla data di cessazione del rapporto di lavoro con questa istituzione scolastica, per trasferimento ad altra istituzione o cessazione del rapporto di lavoro. Successivamente a tale data, la S,V. non sarà più autorizzata ad effettuare alcun tipo di trattamento di dati per conto di questa istituzione scolastica.

Qualunque violazione delle modalità sopra indicate e delle linee guida consegnate con la presente dà luogo a precise responsabilità ai sensi delle norme contenute nel D L.vo 196/03.

IL DIRETTORE DEI SERVIZI GENERALI ED AMMINISTRATIVI

(Responsabile del trattamento)

……

L'ASSISTENTE TECNICO
(Incaricato del Trattamento)

7. NOMINA DELL'INCARICATO DEL TRATTAMENTO DEI DATI PERSONALI (COLLABORATORE SCOLASTICO)

IL DIRETTORE DEI SERVIZI GENERALI ED AMMINISTRATIVI

in qualità di Responsabile del trattamento dei dati personali dell'Istituto;
richiamate le norme di cui gli art. 29 e 30 del D. L.vo 196/03 s. m.i e considerato :

- che i sottoelencati Collaboratori Scolastici, nell'ambito delle loro mansioni compiono attività che possono comprendere il trattamento dei dati personali in occasione della gestione delle comunicazioni telefoniche e a mezzo fax, della duplicazione attraverso fotocopie, del trasporto documenti e posta e del trasferimento fra i diversi uffici della scuola di domande, documenti ed elenchi contenenti dati personali;
- che la nomina a Incaricato non implica l'attribuzione di funzioni ulteriori rispetto a quelle già assegnate al dipendente bensì costituisce un'autorizzazione a trattare dati personalie fornisce istruzioni sulle modalità cui attenersi nel trattamento;
- che pur permanendo obblighi e responsabilità civili e penali dei dipendenti pubblici nell'ambito delle attività d'ufficio, si dispone , sotto vincolo disciplinare, l'obbligo tassativo di attenersi alle istruzioni allegate da osservarsi da parte dei Collaboratori Scolastici, qualora trattino dati personali;

NOMINA

5. **.....**
6. **.....**
7. **.....**

INCARICATI DEL TRATTAMENTI DI DATI PERSONALI

L'incaricato del trattamento dei dati **SI IMPEGNA A :**
in generale a procedere al trattamento dei dati personali nel rispetto dei principi generali di cui all'art. 30 Del D.Lgs. n.196/2003: in particolare i dati devono essere trattati in modo lecito e secondo correttezza; raccolti e registrati per scopi determinati, espliciti e legittimi; i dati devono essere pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;
nello specifico:

I. Impedire l'intrusione nei locali che gli sono stati affidati in custodia da parte di persone non autorizzate secondo quanto stabilito dal Responsabile del trattamento;

II. Impedire il danneggiamento, la manomissione, la sottrazione, la distruzione o la copia di dati nei locali che gli sono stati affidati in custodia da parte di persone non autorizzate secondo quanto stabilito dal Responsabile del Trattamento;
III. Identificare e verificare l'autorizzazione all'accesso ai locali dei soggetti ammessi dopo l'orario di chiusura degli uffici;
IV. a rispettare i divieti di comunicazione e diffusione dei dati trattati nel corso del presente incarico e a non utilizzare i dati, cui abbia accesso, per finalità incompatibili con quelle relative al profilo di appartenenza, ricordando che le operazioni di comunicazione e diffusione di dati sensibili sono possibili quando vi sia una apposita previsione di legge o di regolamento;
V. ad attenersi, nel loro operato, alle istruzioni per lo svolgimento delle operazioni di trattamento allegate alla presente determinazione di nomina;

La presente nomina è a tempo indeterminato e può essere revocata in qualsiasi momento dal Responsabile del trattamento dei dati personali senza preavviso.

La presente nomina si intende automaticamente revocata alla data di cessazione del rapporto di lavoro con questa istituzione scolastica, per trasferimento ad altra istituzione o cessazione del rapporto di lavoro.

E' fatto divieto di comunicazione e diffusione dei dati trattati nel corso del presente incarico, anche per il tempo successivo alla sua cessazione, senza limiti temporali.

Qualunque violazione delle modalità sopra indicate e delle linee guida consegnate con la presente nomina dà luogo a precise responsabilità ai sensi delle norme contenute nel D L.vo 196/03 s.m.i..

In Roma il…….

IL DIRETTORE DEI SERVIZI GENERALI ED AMMINISTRATIVI
(Responsabile del trattamento)

Firma per presa visione dei COLLABORATORI SCOLASTICI
L'incaricato
(firma)
L'incaricato

(firma)

8. DISPOSIZIONI PER IL COLLABORATORE SCOLASTICO INCARICATO DEL TRATTAMENTO

Le misure operative che il Collaboratore scolastico è tenuto ad adottare per garantire la sicurezza dei dati personali sono le seguenti:

A. Collaboratore scolastico in servizio negli uffici di segreteria

I. Effettuare esclusivamente copie fotostatiche di documenti per i quali si è autorizzati;

II. Non lasciare a disposizione di estranei fotocopie inutilizzate o incomplete di documenti che contengono dati personali o sensibili ma accertarsi che vengano sempre distrutte;

III. Non lasciare incustodito il registro contenente gli indirizzi ed i recapiti telefonici del personale e non annotarne il contenuto sui fogli di lavoro;

IV. Non abbandonare la postazione di lavoro per la pausa o altro motivo senza aver provveduto a custodire in luogo sicuro i documenti trattati;

V. Non consentire che estranei possano accedere ai documenti dell'ufficio o leggere documenti contenenti dati personali o sensibili;

VI.

- Segnalare tempestivamente al Responsabile del trattamento la presenza di documenti incustoditi e provvedere temporaneamente alla loro custodia
- Procedere alla chiusura dei locali non utilizzati in caso di assenza del personale.
- Procedere alla chiusura dei locali di segreteria accertandosi che siano state attivate tutte le misure di protezione e che le chiavi delle stanze siano depositate negli appositi contenitori.
- Attenersi alle direttive ricevute e non effettuare operazioni per le quali non si sia stati espressamente autorizzati dal Responsabile o dal Titolare.
- Identificare e verificare l'autorizzazione all'accesso ai locali dei soggetti ammessi dopo l'orario di chiusura

B. Collaboratore scolastico in servizio ai piani

Accertarsi che al termine delle lezioni non restino incustoditi i seguenti documenti segnalandone tempestivamente l'eventuale presenza al responsabile di sede e provvedendo temporaneamente alla loro custodia:

- Registro personale dei docenti
- Registro di classe
- Certificati medici esibiti dagli alunni a giustificazione delle assenze

- Qualunque altro documento contenente dati personali o sensibili degli alunni o dei docenti

Accertarsi che al termine delle lezioni tutti i computer dell'aula di informatica siano spenti e che non siano stati lasciati incustoditi floppy disk, pen drives, cartelle o altri materiali, in caso contrario segnalarne tempestivamente la presenza al responsabile di laboratorio o di sede provvedendo temporaneamente alla loro custodia.
Verificare la corretta funzionalità dei meccanismi di chiusura di armadi che custodiscono dati personali, segnalando tempestivamente al responsabile di sede eventuali anomalie.
Procedere alla chiusura dell'edificio scolastico accertandosi che tutte le misure di protezione dei locali siano state attivate.

IL DIRETTORE DEI SERVIZI GENERALI ED AMMINISTRATIVI

(Responsabile del trattamento

9. NOMINA DELL'INCARICATO DEL TRATTAMENTO DEI DATI PERSONALI (DOCENTI)

Il Dirigente Scolastico Prof. .....Titolare del Trattamento dei Dati Personali gestiti dall'Istituto Scolastico.....

richiamate le norme di cui gli art. 29 e 30 del D. L.vo 196/03 s. m.i e considerato :

- che i sottoelencati Docenti, ivi ricompresi i Docenti esterni incaricati ufficialmente di funzioni nella scuola (esami, corsi, concorsi e attività integrative), nell'ambito delle loro funzioni compiono attività che possono comprendere il trattamento dei dati personali dei dati personali degli alunni necessari allo svolgimento della funzione di istruzione scolastica, per cui è necessario che siano nominati **Incaricati del trattamento dei dati personali**;
- che la nomina a Incaricato non implica l'attribuzione di funzioni ulteriori rispetto a quelle già assegnate al dipendente bensì costituisce un'autorizzazione a trattare dati personali e fornisce istruzioni sulle modalità cui attenersi nel trattamento;
- che pur permanendo obblighi e responsabilità civili e penali dei dipendenti pubblici nell'ambito delle attività d'ufficio, si dispone , sotto vincolo disciplinare, l'obbligo tassativo di attenersi alle istruzioni allegate da osservarsi da parte dei Docenti qualora trattino dati personali.

NOMINA

8. **.....**
9. **.....**
10. **.....**
11. **.....**

INCARICATI DEL TRATTAMENTO DEI DATI PERSONALI

L'incaricato del trattamento dei dati **SI IMPEGNA**:

- a procedere al trattamento dei dati personali nel rispetto dei principi generali di cui all'art. 30 Del D.Lgs. n.196/2003 s.m.i.: in particolare i dati devono essere trattati in modo lecito e secondo correttezza;
- a raccogliere e registrare i dati per scopi determinati, espliciti e legittimi tenendo conto che devono essere pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;
- a rispettare i divieti di comunicazione e diffusione dei dati trattati nel corso del presente incarico e a non utilizzare i dati, cui abbia accesso, per finalità incompatibili con quelle relative al profilo di appartenenza. Si ricorda che le operazioni di comunicazione e diffusione di dati sensibili sono possibili quando vi sia una apposita previsione di legge o di regolamento;
- ad attenersi, nel loro operato, alle istruzioni per lo svolgimento delle operazioni di trattamento allegate alla presente determina.

La presente nomina è a tempo indeterminato e può essere revocata in qualsiasi momento dal Responsabile del trattamento dei dati personali senza preavviso.

Peraltro si intende automaticamente revocata alla data di cessazione del rapporto di lavoro con questa istituzione scolastica, per trasferimento ad altra istituzione o cessazione del rapporto di lavoro. E' fatto divieto di comunicazione e diffusione dei dati trattati nel corso dei presente incarico, anche per il tempo successivo alla sua cessazione, senza limiti temporali.

Qualunque violazione delle modalità sopra indicate e delle linee guida consegnate con la presente dà luogo a precise responsabilità ai sensi delle norme contenute nel D L.vo 196/03.

In Roma il……

IL DIRIGENTE SCOLASTICO (Titolare del Trattamento dei Dati)

Prof. ……

L'incaricato del Trattamento dei Dati per accettazione ……

L’incaricato del Trattamento dei Dati per accettazione .....

L’incaricato del Trattamento dei Dati per accettazione .....

L’incaricato del Trattamento dei Dati per accettazione .....

L’incaricato del Trattamento dei Dati per accettazione .....

L’incaricato del Trattamento dei Dati per accettazione .....

L’incaricato del Trattamento dei Dati per accettazione .....

L’incaricato del Trattamento dei Dati per accettazione .....

10. DISPOSIZIONI PER I DOCENTI INCARICATI DEL TRATTAMENTO

Le misure operative che gli Incaricati sono tenuti ad adottare per garantire la sicurezza dei dati personali sono le seguenti:

I. Gli Incaricati incaricati del trattamento devono attenersi rigorosamente a tutte le regole dettate dal D.L.vo 196/2003 s.m.i. e in particolare hanno l'obbligo di mantenere in ogni caso il dovuto riserbo per le informazioni delle quali si sia venuti a conoscenza nel corso dell'incarico, anche quando sia venuto meno l'incarico stesso (art. 326 del codice penale e art. 28 della legge 241/90);
II. Gli incaricati del trattamento, ai sensi dell'art. 30 del D.L.vo 196/2003 s.m.i., debbono operare sotto la diretta autorità del Titolare del trattamento dei Dati e devono elaborare i dati personali ai quali hanno accesso attenendosi a queste misure operative.

A. FINALITÀ DEL TRATTAMENTO

Si premette che, ai sensi dell'art. 18 del D.L.vo 196/2003 s.m.i., il trattamento di dati personali da parte di soggetti pubblici è consentito soltanto per lo svolgimento delle funzioni istituzionali;

B. MODALITÀ DI TRATTAMENTO DEI DATI

- il trattamento può essere effettuato **manualmente**, mediante **strumenti informatici, telematici o altri supporti** e deve essere applicato il principio **di pertinenza e non eccedenza** rispetto alle finalità del trattamento medesimo, pertanto è consentita l'acquisizione dei soli dati personali strettamente indispensabili per adempiere alle finalità richieste dall'interessato;
- ogni acquisizione di dati deve essere preceduta dall'apposita informativa all'interessato di cui all'art. 13 e 22 del D.L.vo 196/2003 s.m.i., avendo cura nel caso di documenti ritenuti potenzialmente classificabili come sensibili o giudiziari di fare espresso riferimento alla normativa che prevede gli obblighi o i compiti in base alla quale è effettuato il trattamento;
- i dati devono essere trattati in modo **lecito e secondo correttezza,** devono essere **esatti ed aggiornati**;

- è vietata all'incaricato del trattamento dei dati la diffusione e comunicazione dei dati personali trattati che non sia funzionale allo svolgimento dei compiti affidati;
- il trattamento deve essere eseguito osservando le norme di legge in materia di tutela della riservatezza dei dati personali e devono essere applicate le misure di protezione previste dal titolare;

C. CATEGORIE DI SOGGETTI AI QUALI I DATI POSSONO ESSERE COMUNICATI

- La comunicazione da parte della scuola ad altri soggetti pubblici è ammessa quando è prevista da una norma di legge o di regolamento (art. 19 del D.L.vo 196/2003 s.m.i.) e sempre, comunque, previa informazione al Titolare del Trattamento dei Dati.
- I Docenti, prima di procedere alla comunicazione a terzi di qualunque dato personale in loro possesso devono chiedere l'autorizzazione del Titolare del trattamento ;

D. MODALITÀ DI TRATTAMENTO DEI DATI SENSIBILI/GIUDIZIARI

- I documenti (ivi ricompresi quelli non definitivi) ed i supporti recanti dati sensibili o giudiziari devono essere conservati in arredi muniti di serratura e non devono essere lasciati incustoditi in assenza dell'incaricato del trattamento dei dati;

E. TRATTAMENTI DI DATI INERENTI LA SALUTE

- i supporti ed i documenti recanti dati relativi alla salute e alle abitudini sessuali devono essere conservati separatamente in contenitori muniti di serratura.

F. TRATTAMENTO CON SISTEMI INFORMATICI:

- I Docenti non debbono memorizzare dati personali, sensibili o giudiziari sui PC dei laboratori o comunque destinati al supporto dell'attività didattica.

In Roma il……

IL DIRIGENTE SCOLASTICO (Titolare del Trattamento dei Dati)

Prof. ……

L'incaricato del Trattamento dei Dati per accettazione ……

L'incaricato del Trattamento dei Dati per accettazione ……

L'incaricato del Trattamento dei Dati per accettazione ……

L'incaricato del Trattamento dei Dati per accettazione ……

L'incaricato del Trattamento dei Dati per accettazione ……

L'incaricato del Trattamento dei Dati per accettazione ……

L'incaricato del Trattamento dei Dati per accettazione ……

L'incaricato del Trattamento dei Dati per accettazione ……

11. ELENCO DEGLI INCARICATI DEL TRATTAMENTO DEI DATI CHE UTILIZZANO DOTAZIONI INFORMATICHE

Vedi Nomine

Il Dirigente Scolastico
Dott.ssa Maria CANOSA
Firma autografata sostituita a mezzo stampa
ai sensi del D.Lgs 39/1993 art.3 c.25