ISTITUTO D' ISTRUZIONE SUPERIORE
8 MARZO - K. LORENZ
Via Matteotti, 42A/3 - 30035 Mirano - Venezia
CF 90164450273
Tel 041430955 Fax 041434281 veis02800q@istruzione.it veis02800q@pec.istruzione.it www.8marzolorenz.gov.it

Prot. vedi Segnatura *Mirano, vedi Segnatura*

Al docente

.....

SEDE

Oggetto: **Nomina Incaricato al trattamento dei dati personali ai sensi dell'art. 30 D. Lgs. 196/2003 e dell'art. 4 Reg. UE n. 679/2016**

IL DIRIGENTE

- Visto il decreto legislativo n. 196/2003 (Codice in materia di protezione dei dati personali)
- Visto il Regolamento UE n. 679/2016 (G.D.P.R. General Data Protection Regulation)
- Preso atto che l'art. 4 comma 1 lett. h) del d.lgs. n. 196/2003 definisce "incaricati" le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;
- Preso atto che l'art. 4 n. 10) prevede la figura della "persona autorizzata al trattamento" dei dati personali;
- Premesso che il Garante ha statuito che "Le disposizioni del Codice in materia di incaricati del trattamento sono pienamente compatibili con la struttura e la filosofia del regolamento, in particolare alla luce del principio di "responsabilizzazione" di titolari e responsabili del trattamento che prevede l'adozione di misure atte a garantire proattivamente l'osservanza del regolamento nella sua interezza. In questo senso, e anche alla luce degli artt. 28, paragrafo 3, lettera b), 29, e 32, paragrafo 4, in tema di misure tecniche e organizzative di sicurezza, si ritiene opportuno che titolari e responsabili del trattamento mantengano in essere la struttura organizzativa e le modalità di designazione degli incaricati di trattamento" [nota: http://www.garanteprivacy.it/titolare-responsabile-incaricato-del-trattamento]
- Preso atto che l'art. 30 del d. lgs. 196/2003 dispone che:

1. Le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite.

2. La designazione è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito";

- Preso atto che l'art. 29 del Reg. UE 679/2016 dispone che:

"Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri";

- Preso atto che l'art. 32 comma 4 del Reg. UE 67972016 dispone che:

"Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri";

DESIGNA

Il docente.

INCARICATO DEL TRATTAMENTO DEI DATI PERSONALI

in relazione alle operazioni di elaborazione di dati personali, su supporto cartaceo e/o elettronico, ai quali il docente ha accesso nell'espletamento delle funzioni e dei compiti assegnati nell'ambito del rapporto di lavoro con questa istituzione scolastica e disciplinati dalla normativa in vigore e dai contratti di settore. In particolare**, in qualità di Docente** è incaricato delle operazioni di raccolta, registrazione, organizzazione, conservazione, consultazione, modifica, connesse alle seguenti funzioni e attività svolte:

<u>Alunni e genitori</u>

- attività didattica e partecipazione agli organi collegiali;
- valutazione alunni;
- tenuta documenti e registri di attestazione dei voti e di documentazione della vita scolastica dello studente, nonché delle relazioni tra scuola e famiglia quali ad esempio richieste, istanze e corrispondenza con le famiglie;
- in questo quadro: rapporti con famiglie e alunni in situazione di disagio psico-sociale; ricezione di certificati medici relativi allo stato di salute degli alunni, documentazione alunni disabili, documentazione mensa/intolleranze, documentazione DSA e BES, nei limiti sempre di quanto strettamente indispensabile;
- eventuali contributi e/o tasse scolastiche versati da alunni e genitori;
- adempimenti connessi alle visite guidate e ai viaggi d'istruzione;
- conoscenza di dati relativi a professioni di fede religiosa;

Le operazioni sopra descritte vanno rigorosamente effettuate tenendo presenti le istruzioni operative che seguono:

1. il trattamento dei dati personali cui il docente è autorizzato ad accedere, deve avvenire secondo le modalità definite dalla normativa in vigore, in modo lecito e secondo correttezza e con l'osservanza - in particolare - delle prescrizioni di cui al Regolamento UE 2016/679 e al Dlgs 196/2003;
2. il trattamento dei dati personali è consentito soltanto per lo svolgimento delle funzioni istituzionali della scuola;
3. i dati personali, oggetto dei trattamenti, devono essere esatti ed aggiornati, inoltre devono essere pertinenti, completi e non eccedenti le finalità per le quali vengono raccolti e trattati;
4. è vietata qualsiasi forma di diffusione e comunicazione dei dati personali trattati che non sia strettamente funzionale allo svolgimento dei compiti affidati e autorizzata dal responsabile o dal titolare del trattamento. Si raccomanda particolare attenzione a tutela del diritto alla riservatezza degli interessati (persone fisiche a cui afferiscono i dati personali);

5. si ricorda che l'obbligo di mantenere la dovuta riservatezza in ordine alle informazioni delle quali si sia venuti a conoscenza nel corso dell'incarico, deve permanere in ogni caso, anche quando sia venuto meno l'incarico stesso;
6. i trattamenti andranno effettuati rispettando le misure di sicurezza predisposte nell'istituzione scolastica; in ogni operazione di trattamento andrà garantita la massima riservatezza e custodia degli atti e dei documenti contenenti dati personali che non andranno mai lasciati incustoditi o a disposizione di terzi non autorizzati ad accedervi, prendervi visione o ad effettuare qualsivoglia trattamento;
7. le eventuali credenziali di autenticazione (codice di accesso e parola chiave per accedere ai computer e ai servizi web) attribuite alle SS.LL sono personali e devono essere custodite con cura e diligenza; non possono essere messe a disposizione né rivelate a terzi; non possono essere lasciate incustodite, né in libera visione. In caso di smarrimento e/o furto, bisogna darne immediata notizia al responsabile (o, in caso di assenza del responsabile, al titolare) del trattamento dei dati;
8. nel caso in cui per l'esercizio delle attività sopra descritte sia inevitabile l'uso di supporti rimovibili (quali ad esempio chiavi USB, CD-ROM, ecc), su cui sono memorizzati dati personali, essi vanno custoditi con cura, ne messi a disposizione o lasciati al libero accesso di persone non autorizzate;
9. si ricorda inoltre che i supporti rimovibili contenenti dati sensibili e/o giudiziari se non utilizzati vanno distrutti o resi inutilizzabili;
10. si ricorda inoltre che l'accesso agli archivi contenenti dati sensibili o giudiziari è permesso solo alle persone autorizzate e soggetto a continuo controllo secondo le regole definite dallo scrivente;
11. durante i trattamenti i documenti contenenti dati personali vanno mantenuti in modo tale da non essere alla portata di vista di persone non autorizzate;
12. al termine del trattamento occorre custodire i documenti contenenti dati personali all'interno di archivi/cassetti/ armadi muniti di serratura;
13. i documenti della scuola contenenti dati personali non possono uscire dalla sede scolastica, né copiati, se non dietro espressa autorizzazione del responsabile o dal titolare del trattamento;
14. in caso di allontanamento anche temporaneo dal posto di lavoro, o comunque dal luogo dove vengono trattati i dati, l'incaricato dovrà verificare che non vi sia possibilità da parte di terzi, anche se dipendenti non incaricati, di accedere a dati personali per i quali era in corso un qualunque tipo di trattamento;
15. le comunicazioni agli interessati (persone fisiche a cui afferiscono i dati personali) dovranno avvenire in forma riservata; se effettuate per scritto dovranno essere consegnate in contenitori chiusi;
16. all'atto della consegna di documenti contenenti dati personali l'incaricato dovrà assicurarsi dell'identità dell'interessato o di chi è stato delegato al ritiro del documento in forma scritta
17. in caso di comunicazioni elettroniche ad alunni, colleghi, genitori, personale della scuola o altri soggetti coinvolti per finalità istituzionali, queste (comunicazioni) vanno poste in essere seguendo le indicazioni fornite dall'Istituzione scolastica e avendo presente la necessaria riservatezza delle comunicazioni stesse e dei dati coinvolti.

La presente designazione ha validità permanente (per tutto il tempo in cui il docente rimarrà in servizio presso l'Istituto) e pertanto non sarà soggetta a rinnovo annuale.

Il Dirigente Scolastico
Firma apposta ai sensi art. 3 comma 2 D. L.vo 39/1993

Per ricevuta:

ELENCO DEGLI SPECIFICI COMPITI E FUNZIONI ATTRIBUITI E CONNESSI AL TRATTAMENTO DEI DATI PERSONALI
SOTTO IL PROFILO DEL TRATTAMENTO DI DATI PERSONALI:

Nello svolgere le proprie funzioni, che comportino un trattamento di dati personali, il personale scolastico deve attenersi alle seguenti istruzioni:

- in attuazione del principio di «liceità, correttezza e trasparenza»,
- le operazioni di raccolta, registrazione, elaborazione di dati ed in generale, le operazioni di trattamento tutte, avvengono agli esclusivi fini dell'inserimento o arricchimento degli archivi/banche dati della Scuola, nell'osservanza delle tecniche e metodologie in atto;
- autorizzazione a comunicare o eventualmente diffondere o trasferire all'esterno i dati personali esclusivamente ai soggetti autorizzati a riceverli legittimamente, per le finalità per le quali gli stessi sono stati raccolti e comunque nel rispetto delle istruzioni ricevute dal Titolare del trattamento;
- in attuazione del principio di «minimizzazione dei dati», obbligo di trattamento dei soli ed esclusivi dati personali che si rivelino necessari rispetto alle finalità per le quali sono trattati nell'attività a cui è preposto;
- in attuazione del principio di «limitazione della finalità» il trattamento deve essere conforme alle finalità istituzionali del Titolare e limitato esclusivamente a dette finalità;
- in attuazione del principio di «esattezza», obbligo di assicurare l'esattezza, la disponibilità, l'integrità, nonché il tempestivo aggiornamento dei dati personali, ed obbligo di verificare la pertinenza, completezza e non eccedenza rispetto alle finalità per le quali i dati sono stati raccolti, e successivamente trattati;
- in attuazione del principio di «limitazione della conservazione»
- conservare i dati 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 e obbligo di esercitare la dovuta diligenza affinché non vengano conservati, nella Scuola, dati personali non necessari o divenuti ormai superflui. Alla conclusione del trattamento, obbligo di assicurarsi che i documenti contenenti i dati di cui agli articoli 9 e 10 del GDPR vengano conservati in contenitori/armadi muniti di serratura od in ambienti ad accesso selezionato e vigilato, fatte salve le norme in materia di archiviazione amministrativa;
- in attuazione del principio di «integrità e riservatezza» obbligo di garantire un'adeguata sicurezza dei dati personali, compresa la protezione, dando diligente ed integrale attuazione alle misure logistiche, tecniche informatiche, organizzative, procedurali definite dal Titolare, trattando i dati stessi con la massima riservatezza ai fini di impedire trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali. In particolare:
- riporre in archivio, al termine del periodo di trattamento, i supporti ed i documenti, ancorché non definitivi, contenenti i dati personali;
- non fornire dati personali per telefono, qualora non si abbia certezza assoluta sull'identità del destinatario;
- evitare di inviare, per e-mail, documenti in chiaro contenenti dati personali: si suggerisce, in tal caso, di inviare la documentazione, senza alcun esplicito riferimento all'Interessato (ad esempio, contrassegnando i documenti semplicemente con un codice);
- In attuazione del principio di «trasparenza»:
- accertarsi dell'identità dell'Interessato, prima di fornire informazioni circa i dati personali od il trattamento effettuato;
- fornire all'Interessato (o verificare che siano state fornite) tutte le informazioni di cui agli articoli 13 e 14 del GDPR e le comunicazioni di cui agli articoli da 15 a 22 ed all'articolo 34 del GDPR, relative al trattamento utilizzando apposita modulistica. Se richiesto dall'Interessato, le informazioni medesime possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'Interessato;

- agevolare l'esercizio dei diritti dell'Interessato ai sensi degli articoli da 15 a 22 del GDPR;

Le stesse istruzioni e prescrizioni cogenti sono obbligatorie anche per il trattamento di dati personali realizzato, interamente o parzialmente, con strumenti elettronici, contenuti in archivi/banche dati o destinati a figurarvi.

In particolare, per tali trattamenti la persona fisica Autorizzata al trattamento ha l'obbligo di utilizzo e gestione attenendosi alle seguenti istruzioni:

A) Strumenti elettronici in generale

✔ i computer fissi e notebook ed i programmi per elaboratore su di essi installati sono uno strumento di lavoro e contengono dati riservati e informazioni personali di terzi ai sensi della normativa sulla protezione dei dati personali: vanno, pertanto, utilizzati e conservati, insieme ai relativi documenti esplicativi, con diligenza e cura, attenendosi alle prescrizioni fornite dal Titolare e nel rispetto delle indicazioni da questo fornite;

✔ in generale tutti i dispositivi elettronici sono forniti per lo svolgimento della sua attività lavorativa, nell'ambito delle mansioni a questo affidate. L'uso per fini personali è da considerare pertanto eccezionale e limitato a comunicazioni occasionali e di breve durata, ad esclusione dei dispositivi per i quali è esplicitamente regolamentato l'uso per fini personali è importante non lasciare documentazione personale memorizzata nei dispositivi informatici per evitare diffusione della stessa ad altri soggetti;

✔ le impostazioni dei personal computer e dei relativi programmi per elaboratore installati sono predisposte dagli addetti informatici incaricati sulla base di criteri e profili decisi dal Titolare, in funzione della qualifica del dipendente, delle mansioni cui questo è adibito, nonché delle decisioni e della politica di utilizzo di tali strumenti stabilita dalla Scuola. Il dipendente non può modificarle autonomamente; può ottenere cambiamenti nelle impostazioni solo previa autorizzazione.

✔ assicurarsi, in caso di sostituzione del computer utilizzato, che siano effettuate le necessarie operazioni di formattazione o distruzione dei supporti di memorizzazione dei dati;

✔ rivolgersi tempestivamente, per difficoltà o questione inerente alla sicurezza, al Dirigente scolastico o al DPO il dott. Francesco Dei Rossi all'indirizzo mail dpo@dposcuola.com;

✔ per finalità di assistenza, manutenzione ed aggiornamento e previo consenso esplicito del dipendente stesso, l'Amministratore di Sistema o soggetti appositamente incaricati allo svolgimento di tale attività potranno accedere da remoto al personal computer del dipendente attraverso un apposito programma "software" che lo stesso indicherà;

✔ il dipendente è tenuto ad osservare le medesime precauzioni e cautele, ove queste siano applicabili e pertinenti rispetto allo specifico strumento utilizzato, in relazione a tutti i dispositivi elettronici di cui fa uso, tra cui ad esempio fotocopiatrici, scanner, masterizzatori, telefoni fissi, cellulari, pen-drive, cloud e supporti di memoria.

✔ al dipendente è consentito l'utilizzo degli strumenti informatici forniti dalla Scuola per poter assolvere alle incombenze personali senza doversi allontanare dalla sede di servizio, purché l'attività sia contenuta in tempi ristretti e senza alcun pregiudizio per i compiti istituzionali, importante non lasciare nel dispartivo utilizzato documenti e dati personali.

La Scuola ha facoltà di svolgere gli accertamenti necessari e adottare ogni misura atta a garantire la sicurezza e la protezione dei sistemi informatici, delle informazioni e dei dati.

B) Predisposizione di atti e documenti da pubblicare sul sito web istituzionale

Il personale scolastico preposto alla pubblicazione di atti e documenti sul sito istituzionale della Scuola deve:

✔ adottare opportuni accorgimenti prima di procedere alla pubblicazione sul sito internet istituzionale tra cui:

- individuare se esiste un presupposto di legge o di regolamento che legittima la diffusione del documento o del dato personale;

- verificare, caso per caso, se ricorrono i presupposti per l'oscuramento di determinate informazioni;
- verificare che siano sottratti all'indicizzazione (cioè alla reperibilità sulla rete da parte dei motori di ricerca) eventuali categorie particolari di dati (i c.d. dati sensibili) e i giudiziari.

Fermi restando i casi di divieto previsti dalla legge, i dipendenti non possono divulgare o diffondere per ragioni estranee al loro rapporto di lavoro con l'amministrazione e in difformità alle disposizioni di cui al decreto legislativo 13 marzo 2013, n. 33, e alla legge 7 agosto 1990, n. 241, documenti, anche istruttori, e informazioni di cui essi abbiano la disponibilità.

C) Password e username (credenziali di autenticazione informatica)

✔ per le banche dati informatiche, utilizzare sempre il proprio codice di accesso personale, evitando di operare su terminali altrui ed astenendosi dall'accedere a servizi telematici non consentiti. Le credenziali di autenticazione informatica sono individuali. Non possono essere condivise o cedute;

✔ è vietato comunicare a terzi gli esiti delle proprie interrogazioni delle banche dati;

✔ i codici identificativi, le password e le smart card saranno disattivati nel caso in cui i dipendenti cessino il loro rapporto di lavoro, oltre che nei casi espressamente e tassativamente previsti dalla normativa. In tali casi il dipendente è tenuto a restituirle agli uffici a ciò preposti.

✔ la password che la persona fisica designata e autorizzata al trattamento imposta, con il supporto e l'assistenza, in caso di difficoltà, dell'Amministratore di Sistema (se esistente):

- deve essere sufficientemente lunga e complessa e deve contemplare l'utilizzo di caratteri maiuscoli e speciali e numeri (almeno 8 caratteri);
- non deve essere riconducibile alla persona;
- deve essere cambiata almeno ogni 3/6 mesi;
- non deve essere rivelata o fatta digitare al personale di assistenza tecnica;
- non deve essere rivelata o comunicata al telefono, via fax od altra modalità elettronica;

D) Assenza od impossibilità temporanea o protratta nel tempo

✔ nell'ipotesi di assenza o impossibilità, temporanea o protratta nel tempo, del dipendente, qualora per ragioni di sicurezza o comunque per garantire l'ordinaria operatività del Titolare sia necessario accedere ad informazioni o documenti di lavoro presenti sul personal computer del dipendente, inclusi i messaggi di posta elettronica in entrata ed in uscita, il dipendente può delegare a un altro dipendente a sua scelta ("fiduciario") il compito di verificare il contenuto di messaggi e inoltrare quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Di tale attività deve essere redatto apposito verbale e informato il dipendente interessato alla prima occasione utile.

✔ in caso di assenza o impossibilità, temporanea o protratta nel tempo, del dipendente, qualora per ragioni di sicurezza o comunque per garantire l'ordinaria operatività dell'ufficio sia necessario accedere a informazioni o documenti di lavoro presenti sul personal computer del dipendente, inclusi i messaggi di posta elettronica in entrata ed in uscita, ed il dipendente non abbia delegato un suo fiduciario, secondo quanto sopra specificato, il Dirigente scolastico può richiedere con apposita e motivata richiesta all'Amministratore del Sistema di accedere alla postazione e/o alla casella di posta elettronica del dipendente assente, in modo che si possa prendere visione delle informazioni e dei documenti necessari. Contestualmente, il Dirigente scolastico deve informare il dipendente dell'avvenuto accesso appena possibile, fornendo adeguata spiegazione e redigendo apposito verbale.

E) Log-out

✔ In caso di allontanamento anche temporaneo dalla postazione di lavoro (personal computer fisso o notebook o monito interattivo), il dipendente non deve lasciare il sistema operativo aperto con la propria password e/o smart card inserita. Al fine di evitare che persone estranee effettuino accessi non consentiti, il dipendente deve attivare il salvaschermo con password o deve bloccare il computer e togliere la smart card dall'apposito alloggiamento.

F) Utilizzo della rete internet e relativi servizi - Cloud storage

✔ non è consentito navigare in siti web non attinenti allo svolgimento delle mansioni assegnate, soprattutto in quelli che possono rivelare le opinioni politiche, religiose o sindacali del dipendente;

✔ è da evitare la registrazione a servizi on-line, a titolo o per interesse personale;

✔ non è consentita l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo casi direttamente autorizzati e con il rispetto delle normali procedure di acquisto;

✔ non è permessa la partecipazione, per motivi non professionali, a servizi di forum, l'utilizzo di chat-line, di bacheche elettroniche e le registrazioni in guest book anche utilizzando pseudonimi (o nicknames);

✔ il dipendente si impegna a circoscrivere gli ambiti di circolazione e di trattamento dei dati personali (es. memorizzazione, archiviazione e conservazione dei dati in cloud) ai Paesi facenti parte dell'Unione Europea, con espresso divieto di trasferirli in paesi extra UE che non garantiscano (o in assenza di) un livello adeguato di tutela, ovvero, in assenza di strumenti di tutela previsti dal Regolamento UE 2016/679 (Paese terzo giudicato adeguato dalla Commissione Europea, BCR di gruppo, clausole contrattuali modello, consenso degli interessati, etc.).

G) Posta elettronica

✔ la casella di posta elettronica è uno strumento finalizzato allo scambio di informazioni nell'ambito dell'attività lavorativa;

✔ l'utilizzo di account istituzionali è consentito per i soli fini connessi all'attività lavorativa o ad essa riconducibili e non può in alcun modo compromettere la sicurezza o la reputazione della Scuola. L'utilizzo di caselle di posta elettroniche personali è di norma evitato per attività o comunicazioni afferenti al servizio, salvi i casi di forza maggiore dovuti a circostanze in cui il dipendente, per qualsiasi ragione, non possa accedere all'account istituzionale;

✔ si invitano i dipendenti a non utilizzare gli indirizzi di posta elettronica istituzionali assegnati per le comunicazioni personali;

✔ al fine di garantire la continuità all'accesso dei messaggi da parte dei soggetti adibiti ad attività lavorative che richiedono la condivisione di una serie di documenti si consiglia e si incoraggia l'utilizzo abituale di caselle di posta elettronica condivise tra più lavoratori o delle caselle di posta istituzionali della Scuola, eventualmente affiancandoli a quelli individuali;

✔ le comunicazioni via posta elettronica devono avere un contenuto espresso in maniera professionale e corretta nel rispetto della normativa vigente.

✔ non è consentito inviare o memorizzare messaggi di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica o che possano essere in qualunque modo fonte di responsabilità della Scuola;

✔ il dipendente è responsabile del contenuto dei messaggi inviati. I dipendenti si uniformano alle modalità di firma dei messaggi di posta elettronica di servizio individuate dalla Scuola. Ciascun messaggio in uscita deve consentire l'identificazione del dipendente mittente e deve indicare un recapito istituzionale al quale il medesimo è reperibile;

✔ la posta elettronica diretta all'esterno della rete della Scuola può essere intercettata da estranei e, dunque, non deve essere usata per inviare documenti contenenti dati personali di cui agli articoli 9 e 10 del GDPR;

✔ non è consentito l'utilizzo dell'indirizzo di posta elettronica istituzionale della Scuola per la partecipazione a dibattiti, Forum o mail-list, salvo diversa ed esplicita autorizzazione;

✔ qualora si verifichino anomalie nell'invio e ricezione dei messaggi di posta elettronica sarà cura del dipendente informare prontamente l'Amministratore di sistema o il Dirigente scolastico.

H) Software, applicazioni e servizi esterni

✔ onde evitare pericolo di introdurre virus informatici nonché di alterare la stabilità delle applicazioni dell'elaboratore, è consentito installare programmi provenienti dall'esterno solo se espressamente autorizzati dall'Amministratore di sistema o figura analoga ovvero dal Dirigente scolastico.

✔ non è consentito utilizzare strumenti software e/o hardware atti ad intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;

✔ non è consentito modificare le configurazioni impostate sul proprio PC;

✔ non è consentito configurare gli strumenti per la gestione della posta elettronica per la gestione di account privati. Non è inoltre consentito utilizzare detti strumenti per la ricezione, visualizzazione ed invio di messaggi a titolo personale;

✔ il Titolare si riserva la facoltà di procedere alla rimozione di ogni file od applicazione che riterrà essere pericolosi per la sicurezza del sistema ovvero acquisiti od installati in violazione delle presenti istruzioni;

✔ tutti i software caricati sul sistema operativo ed in particolare i software necessari per la protezione dello stesso o della rete internet (quali antivirus o firewall) non possono essere disinstallati o in nessun modo manomessi, (salvo quando questo sia richiesto dall'amministratore di sistema per compiere attività di manutenzione o aggiornamento).

I) Reti di comunicazione

✔ nel caso di trattamento di dati personali effettuato mediante elaboratori non accessibili da altri elaboratori (cioè mediante computer stand alone) è necessario utilizzare la parola chiave (password) fornita per l'accesso al singolo PC;

✔ nel caso di trattamento di dati personali effettuato mediante elaboratori accessibili da altri elaboratori, solo in rete locale, o mediante una rete di telecomunicazioni disponibili al pubblico, è necessario: utilizzare la parola chiave (password) fornita per l'accesso ai dati, oltre a servirsi del codice identificativo personale per l'utilizzazione dell'elaboratore;

✔ le unità di rete o lo spazio all'interno del Registro elettronico sono aree di condivisione di informazioni strettamente professionali e non possono, in alcun modo, essere utilizzate per scopi diversi. Pertanto, qualunque "file" che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità;

✔ al fine di garantire la disponibilità dei documenti di lavoro assicurandone il backup periodico, si dovrà procedere al loro salvataggio nell'apposita area di rete individuale o di gruppo a ciò dedicata e disponibile sui sistemi server del Titolare;

✔ non collegare dispositivi che consentano un accesso, non controllabile, ad apparati della rete del Titolare.

✔ non condividere file, cartelle, hard-disk o porzioni di questi del proprio computer, per accedere a servizi non autorizzati di peer to peer al fine condividere materiale elettronico tutelato dalle normative sul diritto d'autore (software, file audio, film, etc.).

J) Utilizzo dei mezzi di informazione e dei social media

✔ nell'utilizzo dei propri account di social media, il dipendente utilizza ogni cautela affinché le proprie opinioni o i propri giudizi su eventi, cose o persone, non siano in alcun modo attribuibili direttamente alla Scuola di appartenenza;

✔ in ogni caso il dipendente è tenuto ad astenersi da qualsiasi intervento o commento che possa nuocere al prestigio, al decoro o all'immagine della Scuola;

✔ al fine di garantirne i necessari profili di riservatezza le comunicazioni, afferenti direttamente o indirettamente il servizio non si svolgono, di norma, attraverso conversazioni pubbliche mediante l'utilizzo di piattaforme digitali o social media. Sono escluse da tale

limitazione le attività o le comunicazioni per le quali l'utilizzo dei social media risponde ad una esigenza di carattere istituzionale.

K) Supporti esterni di memorizzazione

La persona fisica designata e autorizzata al trattamento, ha l'obbligo di:

- utilizzare i supporti di memorizzazione solamente qualora i dati in essi precedentemente contenuti non siano in alcun modo recuperabili, altrimenti etichettarli e riporli negli appositi contenitori;
- proteggere i dati personali archiviati su supporti esterni con le stesse misure di sicurezza previste per i supporti cartacei;
- verificare che i contenitori degli archivi/banche dati (armadi, cassettiere, computer, etc.) vengano chiusi a chiave e/o protetti da password in tutti i casi di allontanamento dalla postazione di lavoro;
- evitare che i dati estratti dagli archivi/banche dati possano divenire oggetto di trattamento illecito;
- copie di dati personali su supporti amovibili sono permesse solo se parte del trattamento; copie di dati contemplati dagli articoli 9 e 10 del GDPR devono essere espressamente autorizzate. In ogni caso tali supporti devono avere un'etichetta che li identifichi e non devono mai essere lasciati incustoditi;
- evitare di asportare supporti informatici o cartacei contenenti dati personali di terzi, senza la previa autorizzazione.
- procedere alla cancellazione dei supporti esterni contenenti dati personali, prima che i medesimi siano riutilizzati. Se ciò non è possibile, essi devono esser distrutti;
- verificare l'assenza di virus nei supporti utilizzati.