ISTITUTO D'ISTRUZIONE SUPERIORE "L. NOSTRO - L. REPACI"
VILLA SAN GIOVANNI RC
Via Garibaldi, 75 – 89018 – Villa San Giovanni (RC) - C. M. RCIS03600Q
Tel. /Fax 0965/499481 www.nostrorepaci.edu.it
e-mail rcis03600q@istruzione.it - pec rcis03600q@pec.istruzione.it

POLICY E ISTRUZIONI SUL TRATTAMENTO DEI DATI PERSONALI

ai sensi del Regolamento Europeo sulla Protezione dei Dati 2016/679

INDICE

1. SCOPO DEL DOCUMENTO

Attraverso questo documento il titolare del trattamento, **l'Istituto d'Istruzione Superiore "L. Nostro – L. Repaci"**, vuole fornire al personale scolastico le istruzioni relative al trattamento dei dati nonché fare chiarezza in merito a tutti i soggetti coinvolti nel trattamento degli stessi, alle categorie di dati acquisiti dalla scuola e alle misure tecniche organizzative adottate per garantire un'adeguata sicurezza.

2. NORMATIVA DI RIFERIMENTO

- Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio Europeo del 27 Aprile 2016 (protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE), entrato in vigore il 25 maggio 2018;
- Decreto legislativo 196/2003 così come modificato dal decreto legislativo 101/2018 entrato in vigore il 19.09.2018 (disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento europeo 2016/679).

3. I DATI

I dati, ai sensi dell'articolo 4 del GDPR, sono qualsiasi informazione concernente una persona fisica identificata (es. il nome) o identificabile anche indirettamente e perciò anche un'informazione riguardante una persona, la cui identità può comunque essere accertata mediante informazioni supplementari (es. il codice fiscale, l'impronta digitale, l'immagine).

Tutti i dati che riguardano un individuo godono della tutela del GDPR, ma non tutti i dati sono uguali.

Esistono dati comuni, categorie particolari di dati e dati giudiziari.

Categorie particolari di dati (art. 9 GDPR)

- Dati di origine razziale o etnica
- Dati riguardanti le opinioni politiche
- Dati relativi alle convinzioni religiose o filosofiche
- Dati di appartenenza sindacale
- Dati genetici
- Dati biometrici intesi a identificare in modo univoco una persona fisica
- Dati inerenti la salute o l'orientamento sessuale della persona

Dati giudiziari (art. 10 GDPR)

1. Dati relativi a condanne penali
2. Dati riguardanti i reati
3. Dati inerenti all'applicazione di misure di sicurezza

Il trattamento di particolari categorie di dati e i dati relativi a reati o misure di sicurezza in ambito scolastico trovano valido riferimento nel DM 305/2006.

4. I SOGGETTI CHE TRATTANO DATI A SCUOLA

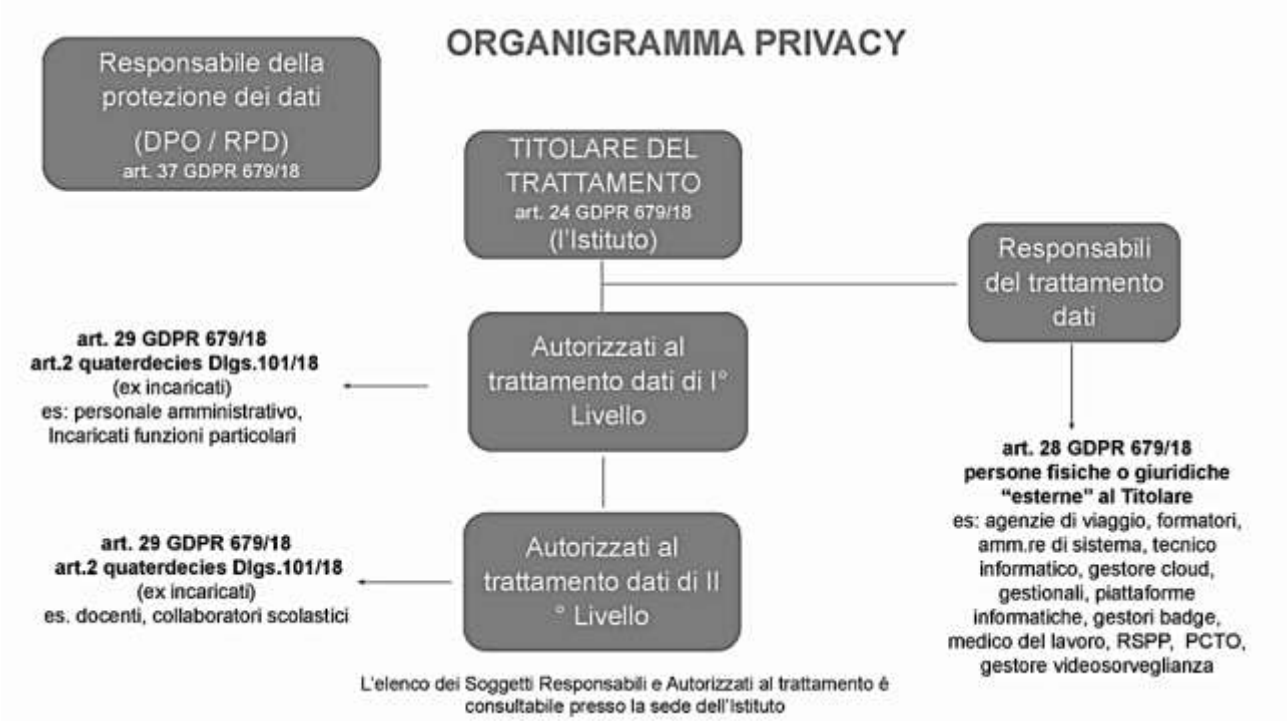
Ogni dipendente scolastico può trattare dati personali di tutti i soggetti con i quali l'istituzione scolastica entra in relazione per i suoi fini istituzionali, nella misura e nei limiti previsti dal profilo di appartenenza e dai compiti contrattuali per esso previsti, nonché da eventuali mansioni attribuite dal dirigente scolastico al singolo soggetto su specifico incarico, nel rispetto della normativa del codice della privacy e del GDPR.

In ogni caso il Titolare del trattamento provvede con apposita nomina a designare il personale scolastico autorizzato al trattamento dei dati e fornisce le istruzioni in merito al trattamento degli stessi. Il personale autorizzato sottoscrive la nomina attraverso il Registro Elettronico apponendo la spunta su "Conferma/Firma". I soggetti che trattano dati all'interno della presente istituzione scolastica sono:

TITOLARE DEL TRATTAMENTO DEI DATI	Titolare del trattamento è l'Istituzione Scolastica in persona del dirigente scolastico. Il titolare è colui che tratta i dati senza ricevere istruzioni da altri, decide "perché" e "come" devono essere trattati i dati. Il titolare del trattamento non è, quindi, chi gestisce materialmente i dati, ma chi decide il motivo e le modalità del trattamento.
CONTITOLARE DEL TRATTAMENTO	Due o più titolari operano come contitolari del trattamento qualora determinano congiuntamente finalità e mezzi del trattamento medesimo (Ministero dell'Istruzione e Scuola).
RESPONSABILE DELLA PROTEZIONE DEI DATI (RPD o DPO)	L'RPD è un consulente esperto che affianca il titolare del trattamento nella gestione delle problematiche del trattamento dei dati personali. Tale designazione è obbligatoria per le amministrazioni e per gli enti pubblici.
RESPONSABILI ESTERNI DEL TRATTAMENTO	Responsabile esterno del trattamento è una persona fisica o giuridica distinta dal titolare che elabora dati per conto di questo, è quindi un soggetto esterno. Ogni fornitore di servizi scolastici rilevanti (ad esempio: per il registro elettronico, gestione documentale, etc.) deve essere nominato responsabile esterno del trattamento dati. Il responsabile deve trattare dati attenendosi alle istruzioni del titolare, assume responsabilità proprie e ne risponde alle autorità di controllo e alla magistratura.
PERSONE AUTORIZZATE AL TRATTAMENTO DEI DATI	D.S.G.A., assistenti amministrativi, assistenti tecnici, corpo docenti e personale collaboratore scolastico. Sono le persone fisiche che effettuano materialmente le operazioni di trattamento sui dati personali. Gli autorizzati possono operare alle dipendenze del titolare o collaborare con il medesimo. Ovviamente gli autorizzati possono essere organizzati con diversi livelli di delega. L'autorizzato è un mero esecutore di compiti e deve attenersi, strettamente, alle istruzioni ricevute dal titolare. Ai sensi dell'art. 2-quaterdecies del Codice della privacy il titolare del trattamento deve individuare le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la loro autorità diretta.
INTERESSATO AL TRATTAMENTO	L'interessato è persona fisica a cui si riferiscono i dati personali

ORGANIGRAMMA

L'Organigramma Privacy riassume e visualizza le differenti figure del Responsabile per la Protezione dei Dati Personali (RPD/DPO), del Titolare del trattamento e soggetti Responsabili ed Autorizzati al trattamento, secondo i ruoli, compiti e responsabilità previsti dalla normativa vigente.



5. IL TRATTAMENTO DEI DATI

Per "trattamento dei dati" si intende qualsiasi attività effettuata sui dati personali: raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, uso, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione o distruzione (art. 4 GDPR).

Elemento identificativo del trattamento è la finalità, che costituisce lo scopo effettivo per il quale i dati vengono raccolti e gestiti.

A ciascuna finalità deve necessariamente corrispondere uno specifico trattamento.

6. ACCESSO AI LUOGHI IN CUI SI EFFETTUANO I TRATTAMENTI

L'accesso ai locali in cui si trovano le apparecchiature informatiche dell'istituzione scolastica (server di rete, computer, stampanti, ecc.) utilizzati per il trattamento dei dati personali, nonché l'accesso agli archivi e ai registri cartacei contenenti dati personali, è controllato ed è permesso esclusivamente al personale debitamente incaricato e autorizzato.

I locali ad accesso controllato sono chiusi anche se presidiati. Dopo l'uscita dell'ultimo incaricato/addetto al trattamento dei dati i locali sono chiusi a chiave.

Eventuali visitatori occasionali delle aree ad accesso controllato sono previamente autorizzati dal Responsabile del trattamento dei dati e accompagnati da un incaricato, che controllerà che i visitatori non accedano a dati in possesso dell'istituzione scolastica se non previamente autorizzati e incaricati.

7. LA CONSERVAZIONE DEI DATI

I dati personali trattati saranno conservati presso gli archivi della scuola per tutta la durata del rapporto tra l'interessato e l'istituzione scolastica, per l'espletamento di tutti gli adempimenti di legge e per un tempo non superiore agli scopi per i quali sono stati raccolti. In ogni caso i dati sono conservati secondo le indicazioni delle Regole tecniche in materia di conservazione digitale degli atti definite da AGID e nei tempi e nei modi indicati dalle Linee Guida per le Istituzioni scolastiche e dai Piani di conservazione e scarto degli archivi scolastici definiti dalla Direzione Generale degli Archivi presso il Ministero dei Beni Culturali.

8. DIRITTI DELL'INTERESSATO

La normativa attribuisce specifici diritti all'interessato, il quale, per l'esercizio di tali diritti, può rivolgersi direttamente al titolare del trattamento.

I diritti esercitabili dall'interessato sono i seguenti:

- diritto di revocare il consenso in qualsiasi momento (nei casi previsti dal GDPR);
- diritto di ottenere informazioni su quali dati sono trattati dal titolare (diritto di informazione);
- diritto di chiedere ed ottenere i dati in possesso del titolare (diritto di accesso);
- esercitare l'opposizione al trattamento in tutto o in parte;
- diritto di opporsi ai trattamenti automatizzati;
- ottenere la cancellazione dei dati in possesso del titolare;
- ottenere l'aggiornamento o la rettifica dei dati conferiti;
- chiedere e ottenere trasformazione in forma anonima dei dati;
- chiedere e ottenere il blocco o la limitazione dei dati trattati in violazione di legge e quelli dei quali non è più necessaria la conservazione in relazione agli scopi del trattamento;
- diritto alla portabilità dei dati.

L'interessato ha inoltre la facoltà di proporre una segnalazione e un reclamo avanti all'Autorità di controllo dello Stato di residenza (Garante per la protezione dei dati personali).

9. INDICAZIONI OPERATIVE PER IL TRATTAMENTO DEI DATI PERSONALI

Il legislatore europeo all'articolo 5 del GDPR fissa i principi applicabili al trattamento dei dati personali. Il titolare del trattamento e tutti i soggetti che trattano dati in suo nome e conto devono pertanto rispettare e applicare i seguenti principi:

- **Liceità, correttezza e trasparenza del trattamento**. Liceità: il trattamento dei dati deve essere rispettoso delle disposizioni del Regolamento e delle Carte sovranazionali e nazionali dei diritti dell'uomo e del cittadino e delle altre norme di legge. Correttezza: il titolare non deve violare norme di legge o commettere abusi nel trattamento dei dati. Trasparenza: chiarezza negli obblighi informativi nei confronti dell'interessato.

- **Limitazione delle finalità**. I dati devono essere raccolti per finalità determinate, esplicite e legittime (pertanto il titolare dovrà assicurare che eventuali trattamenti successivi non siano incompatibili con le finalità della raccolta dei dati)

- **Minimizzazione dei dati**. I dati raccolti devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per cui sono trattati.

- **Esattezza.** I dati trattati devono essere esatti e se necessario aggiornati (compresa la tempestiva cancellazione dei dati che risultino inesatti rispetto alle finalità del trattamento).

- **Limitazione della conservazione**. I dati devono essere conservati per un tempo non superiore a quello necessario rispetto agli scopi per i quali è stato effettuato il trattamento (una volta conseguite le finalità di trattamento i dati vanno eliminati o anonimizzati).

- **Integrità e riservatezza**. I dati devono essere trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentale.

- **Responsabilizzazione**. Il titolare del trattamento dei dati è competente per il rispetto di tutti i principi sopra descritti e deve essere in grado di comprovarlo.

10. MODALITÀ RELATIVE AL TRATTAMENTO DEI DATI

Ogni dipendente scolastico deve trattare i dati personali in modo lecito, corretto e trasparente rispettando le seguenti indicazioni:

- raccogliere e registrare i dati personali per finalità determinate, esplicite e legittime, e i dati raccolti devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per cui sono trattati;
- verificare che siano esatti e, se necessario, aggiornarli;
- verificare che siano pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti e successivamente trattati;
- conservarli in modo sicuro e per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti e successivamente trattati;
- non trasferire a un paese terzo o a un'organizzazione internazionali i dati personali;
- verificare che sia stata RESA l'informativa agli interessati, ai sensi degli artt. 13 e 14 del Regolamento Ue 2016/679;
- non comunicare a terzi, al di fuori dell'ambito lavorativo, o in difformità dalle istruzioni ricevute, qualsivoglia dato personale;
- informare prontamente il Titolare del trattamento di ogni circostanza idonea a determinare pericolo di dispersione o utilizzazione non autorizzata dei dati stessi;
- informare prontamente il Titolare del trattamento qualora si verificasse la necessità di porre in essere operazioni di trattamento di dati personali per finalità o con modalità diverse da quelle risultanti dalle istruzioni ricevute, nonché di ogni istanza di accesso ai dati personali da parte di soggetti interessati e di ogni circostanza che esuli dalle istruzioni impartite;
- accedere solo ai dati strettamente necessari all'esercizio delle proprie funzioni;
- accertarsi dell'identità degli interessati e della loro autorizzazione al trattamento e dell'eventuale autorizzazione scritta a terzi, al momento del ritiro di documentazione in uscita;
- non fornire telefonicamente o a mezzo mail dati e informazioni ai diretti interessati, senza avere la certezza della loro identità;
- non diffondere fotografie o copie di documenti interni dell'istituzione scolastica che devono rimanere riservati;
- non effettuare fotografie, registrazioni vocali e video agli studenti per diffonderli, anche ai genitori, senza il consenso degli interessati e l'autorizzazione del titolare del trattamento;

- seguire le attività di formazione organizzate dalla istituzione scolastica;
- partecipare alla attività di verifica affinché le misure di sicurezza vengano applicate nell'Istituto.
- porre attenzione alla compilazione dei "Registri di classe d'emergenza", cartacei, tenuti in classe sulla scrivania e affidati all'insegnante in servizio rammentando che i dati personali da inserire sono solo quelli necessari ai fini della sicurezza (es. non devono essere riportati dati disciplinari, sanitari, ecc.)
- trasmettere al più presto in Segreteria in busta chiusa I certificati medici o documentazione contenente dati personali consegnati dagli alunni;
- non fotocopiare/scannerizzare documenti contenenti dati personali senza l'autorizzazione del responsabile o del titolare del trattamento;
- non esportare, neppure in forma telematica, documenti o copie contenenti dati personali all'esterno dell'Istituto, senza autorizzazione del titolare o del responsabile del trattamento;
- custodire in sotto-fascicoli chiusi con dicitura "riservato". I dati sensibili separatamente dai dati comuni;
- custodire in armadi e/o cassetti chiusi a chiave i documenti contenenti dati sensibili e giudiziari.

10.1 TRATTAMENTO DEI DATI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

Per "non elettronici" si intendono prioritariamente i documenti cartacei. I documenti di questo tipo contenenti dati particolari (ex dati sensibili) o giudiziari devono essere protetti in appositi armadi dotati di chiavi. Tutti i documenti contenenti dati particolari (ex dati sensibili) o giudiziari, che si ritiene debbano essere eliminati, devono essere distrutti e non gettati nei cestini.

Per proteggere i dati personali è opportuno evitare il deposito di documenti di qualsiasi genere negli ambienti di transito o pubblici (corridoi o sale riunioni), come pure l'abbandono in vista sulle scrivanie quando ci si debba assentare dal proprio posto di lavoro. Nel caso di dati particolari (ex dati sensibili) e/o giudiziari, il rispetto di queste norme è obbligatorio.

Istruzioni specifiche:

a. Distruzione delle copie cartacee

Coloro che sono preposti alla duplicazione di documentazione cartacea o digitale (con stampanti o fotocopiatrici o altre periferiche) sono tenuti a procedere alla relativa distruzione del supporto, qualora si verifichino errori o la riproduzione non sia corretta, evitando di riutilizzare i fogli.

È fatto divieto di trasporto e di copia, al di fuori della sede scolastica, dei documenti contenenti dati personali, se non dietro espressa autorizzazione del Titolare del trattamento.

È altresì obbligatoria l'autorizzazione preventiva, da parte del titolare del trattamento, al possesso di copie (cartacee o digitali) contenenti Piani Didattici Personalizzati e Piani Educativi Individuali, in ogni caso prive dei dati personali che possano consentire l'individuazione dell'alunno.

b. Misure di sicurezza

Il trattamento sicuro di documenti contenenti Dati Personali richiede la presenza di misure di sicurezza con le quali l'Incaricato possa interagire e una serie di accorgimenti direttamente gestibili dall'Incaricato stesso. In particolare, si richiede:

• la presenza e l'uso tassativo di armadi e cassetti dotati di serratura adeguata;

• la presenza e l'uso tassativo, ove si richieda la distruzione di documenti contenenti dati particolari (ex dati sensibili) e giudiziari, di un trita-documenti.

c. Prescrizioni per gli incaricati

L'Incaricato deve attenersi alle seguenti prescrizioni:

- in nessun caso è concesso l'accesso a documentazione contenente Dati Personali per motivi non dettati da esigenze di lavoro strettamente connesse ai trattamenti dichiarati, autorizzati e tutelati dal Titolare;
- la documentazione contenente Dati Personali, che, per ragioni di praticità operativa risiede sulle scrivanie degli Incaricati, deve comunque essere rimossa al termine dell'orario di lavoro;
- l'accesso ai supporti deve essere limitato al tempo necessario a svolgere i Trattamenti previsti;
- i supporti devono essere archiviati in ambiente ad accesso controllato;
- i documenti contenenti dati personali, non devono essere lasciati incustoditi in un ambiente non controllato (ad es. a seguito della stampa dei documenti su stampante di rete);
- il numero di copie di documenti contenenti Dati Personali deve essere strettamente funzionale alle esigenze di lavoro;
- cassetti ed armadi contenenti documentazione riservata debbono tassativamente essere chiusi a chiave fuori dell'orario di lavoro;
- l'accesso fuori orario lavorativo a documenti contenenti Dati particolari (ex dati sensibili) /giudiziari può avvenire da parte di personale Incaricato, o tramite autorizzazione di quest'ultimo, unicamente previa registrazione dell'accesso a tali documenti;
- la distruzione di documenti contenenti Dati Personali deve essere operata, ove possibile, direttamente dal personale Incaricato;
- ove non siano disponibili strumenti per la distruzione dei documenti (trita documenti), o il volume di questi sia tale da imporre il ricorso al servizio di macero, il personale Incaricato che avvia al macero la documentazione è tenuto a confezionare tale documentazione in modo che il pacco risulti anonimo e solido;
- quando gli atti e i documenti contenenti dati personali, dati particolari (ex dati sensibili) o giudiziari sono affidati agli Incaricati per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli Incaricati fino alla restituzione, in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate;
- l'accesso agli archivi contenenti dati particolari (ex dati sensibili) o giudiziari deve essere controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono devono essere preventivamente autorizzate.
- è severamente vietato utilizzare documenti contenenti Dati personali, dati particolari (ex dati sensibili) o giudiziari come carta da riciclo o da appunti.

10.2 TRATTAMENTO DEI DATI CON SISTEMI INFORMATICI

Istruzioni specifiche per l'utilizzo del pc, di sistemi informatici, gestione password ed email

- Custodire in modo appropriato Il personal computer (fisso o mobile) ed i relativi programmi e/o applicazioni affidati al dipendente quali strumenti di lavoro;
- Utilizzare il personal computer ed i relativi programmi e/o applicazioni affidati solo per fini professionali (in relazione, ovviamente alle mansioni assegnate) e non per scopi personali, tanto meno per scopi illeciti; debbono essere prontamente segnalati al titolare del trattamento il furto, danneggiamento o smarrimento di tali strumenti;
- Non lasciare supporti di memoria informatici (chiavette USB, DVD, ecc.), cartelle o altri documenti contenenti dati personali e/o sensibili a disposizione di estranei;

- Non lasciare aperta la sessione di lavoro con la propria password inserita, in caso di allontanamento anche temporaneo dal posto di lavoro, al fine di evitare trattamenti non autorizzati e di consentire sempre l'individuazione dell'autore del trattamento;
- Spegnere correttamente il computer al termine di ogni sessione;
- Cambiare periodicamente (almeno una volta ogni 3 mesi in caso di trattamento di dati di categorie particolari o dati relativi a reati e condanne penali, altrimenti ogni 6 mesi) la propria password o qualora si ritenga compromessa, e scegliere una password con le seguenti caratteristiche: originale, composta da almeno otto caratteri, che contenga almeno un numero, che non sia facilmente intuibile (evitando il nome proprio, il nome di congiunti, date di nascita e comunque riferimenti alla propria persona o lavoro facilmente ricostruibili);
- Curare la conservazione della propria password (tra cui quella per accedere al registro elettronico) ed evitare di comunicarla ad altri;
- Non rivelare ad alcuno le credenziali di accesso al sistema informatico, di propria iniziativa, o dietro richiesta;
- Non scrivere la password in nessun posto in cui possa essere letta facilmente, soprattutto vicino al computer;
- Non utilizzare la posta elettronica della scuola per motivi non attinenti allo svolgimento delle mansioni assegnate;
- Verificare attentamente i destinatari del messaggio di posta elettronica prima dell'invio;
- In caso di utilizzo di posta elettronica, non aprire i documenti di cui non sia certa la provenienza e controllare accuratamente l'indirizzo dei destinatari prima di inviare email contenenti, in allegato o nel corpo del messaggio, dati personali;
- Inviare messaggi di posta solo se espressamente autorizzati;
- Nella comunicazione multimediale per fini istituzionali con alunni e genitori utilizzare esclusivamente le piattaforme informatiche messe a disposizione dall'Istituto; è fatto divieto utilizzare social network;
- Per l'attività didattica utilizzare le piattaforme informatiche approvate dall'Istituto.

Attenzione: Il mancato rispetto di quanto sopra riportato e in particolare dell'obbligo di segretezza e di riservatezza potrà comportare gravi responsabilità amministrative e civili a carico dell'Istituto e del soggetto inadempiente.

Relativamente all'utilizzo di strumenti informatici è stato redatto dal Titolare del Trattamento il documento "Istruzioni per l'utilizzo di strumenti informatici", pubblicato sul sito web dell'Istituzione scolastica, sezione Privacy, che tutto il personale dell'Istituto è tenuto a seguire.

10.3 TRATTAMENTO DEI DATI SU DISPOSITIVI DIGITALI (BYOD) PERSONALI

Premesso che:

Non è consentito l'utilizzo del device/smartphone personale durante le ore di lavoro per motivi non inerenti le attività didattiche, se non in casi di comprovata necessità e se preventivamente autorizzati dal Dirigente scolastico.

Non è consentito, altresì, il collegamento alla rete wi-fi istituzionale tramite strumenti personali se non debitamente autorizzati.

Istruzioni specifiche:

- i suddetti dispositivi devono essere sottoposti a tutte le misure di sicurezza previste per gli strumenti di lavoro di cui al paragrafo 10.2;
- occorre prevedere la creazione di un account dedicato sul proprio personal computer/tablet.
- al fine di monitorare e garantire la sicurezza informatica interna, l'istituto può svolgere verifiche anche su tali dispositivi; eventuali controlli saranno svolti in presenza del proprietario e utilizzatore del bene e saranno limitati alla sola area utilizzata per mansione lavorativa.
- l'utilizzatore è tenuto a informare tempestivamente il dirigente ed il responsabile di eventuali anomalie o alert riscontrati nello strumento durante il suo utilizzo per fini lavorativi.

11. TRATTAMENTO DEI DATI SU STRUMENTI DI ARCHIVIAZIONE (STORAGE HW / SW)

Istruzioni specifiche:

L'utilizzo di sistemi di personal storage (Dropbox, iCloud, Google Drive, Wetransfer) o di supporti rimovibili (hard disk esterni, supporti USB chiavette, CD e DVD riscrivibili) deve essere espressamente autorizzato dal Dirigente Scolastico.

Inoltre:

- ancorché autorizzati, agli utenti è consentito l'utilizzo dei dispositivi rimovibili condizionato alla predisposizione preventiva degli stessi con tecniche crittografiche;
- è consentito caricare sul o sui dispositivi rimovibili e sui sistemi di personal storage solamente i dati essenziali allo svolgimento del proprio lavoro;
- in caso di furto o smarrimento di dispositivi rimovibili, gli utenti hanno l'obbligo di avvisare immediatamente il Titolare del Trattamento;
- se un utente sospetta che sia stato effettuato un accesso non autorizzato ai dati, ha il dovere di riferirlo immediatamente;
- è preferibile dotare i dispositivi in parola di adeguate procedure di autenticazione (es: password per l'accesso alle informazioni);
- è proibito scaricare sui dispositivi in dotazione copie pirata di software o contenuti illegali;
- supporti magnetici o tabulati, contenenti dati sensibili devono essere custoditi in archivi o in cassetti chiusi a chiave;
- lo smaltimento dei supporti rimovibili deve essere affidato al responsabile informatico, che provvederà alla preventiva bonifica dello stesso.

12. TRATTAMENTO DATI DA PARTE ADDETTI ALLA MANUTENZIONE

L'accesso ai dati trattati elettronicamente da parte degli incaricati e degli addetti esterni alla manutenzione è possibile solo in seguito ad autorizzazione scritta del Responsabile del trattamento dati.

La manutenzione degli elaboratori, che preveda o meno il trasferimento fisico presso un laboratorio di riparazioni, è autorizzata solo a condizione che il fornitore del servizio abbia sottoscritto l'accordo con il Titolare per le modalità di trattamento dei dati personali (art. 28 GDPR) e, pertanto, si impegni al rispetto della normativa sulla protezione dei dati personali; il fornitore si deve altresì impegnare a mantenere la dovuta riservatezza in ordine ai dati di cui sia venuto a conoscenza e a non utilizzarli fuori dai casi consentiti, così come previsto dall'accordo con l'istituto.

Le seguenti istruzioni devono essere osservate dai preposti in qualità di addetti alla gestione o manutenzione che trattano dati di titolarità per i quali è nominato un responsabile del trattamento nonché dagli addetti di ditte specializzate che svolgano interventi tecnici di gestione e manutenzione degli strumenti elettronici:

- effettuare operazioni di manutenzione e supporto per verifica corretto funzionamento (monitoraggio e diagnostica) su flussi dei dati;
- gestire le credenziali di autenticazione dei soggetti incaricati del trattamento su indicazione dell'Amministratore di sistema;
- gestire i profili di autorizzazione degli incaricati al trattamento dei dati, su specifiche impartite dai responsabili di funzione/BU, su indicazione dell'Amministratore di sistema;
- provvedere alla disattivazione/variazione delle utenze, ivi compreso l'account di posta elettronica, assegnate al personale cessato dal servizio o che abbia modificato il proprio ambito di trattamento, su richiesta specifica dei responsabili ovvero della Direzione Risorse Umane e su indicazione dell'Amministratore di sistema;
- custodire la documentazione cartacea, prodotta nello svolgimento dei propri compiti istituzionali;

L'accesso agli addetti alla gestione e manutenzione è consentito unicamente ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere alle operazioni di manutenzione dei programmi o del sistema informatico.

A ciascun addetto alla manutenzione, previa sottoscrizione di apposito atto per accettazione, è pertanto consentito eseguire le operazioni strettamente necessarie a tali scopi e/o richieste dal titolare, secondo le seguenti istruzioni operative:

- nel caso in cui sia necessario effettuare stampe di prova per controllare il funzionamento di stampanti o per verificare il funzionamento di strumenti o programmi installati, non utilizzare files già esistenti ma creare files di prova.
- nel caso si renda strettamente necessario accedere a files contenenti dati (ad esempio per il recupero di un testo) limitare l'accesso ai dati per il tempo strettamente necessario all'assolvimento delle operazioni di manutenzione.
- per effettuare operazioni di manutenzione sui database dell'istituto che prevedano la raccolta e la conservazione dei dati, tali dati dovranno essere custoditi in modo tale da non essere accessibili da soggetti non autorizzati.
- devono inoltre essere adottate le misure di sicurezza minime previste dal codice in materia di protezione dei dati personali;
- è necessario informare al più presto il titolare o il responsabile del trattamento qualora si dovessero riscontrare malfunzionamenti o non conformità;
- tutti i dati personali contenuti nei data base devono essere protetti da password.

Nel caso in cui sia necessario accedere ai dati attraverso gli strumenti elettronici in dotazione agli incaricati, attenersi alle seguenti indicazioni:

- in presenza dell'incaricato, far digitare la password dall'incaricato stesso evitando di venirne a conoscenza;
- in assenza dell'incaricato rivolgersi alla persona individuata dall'incaricato quale proprio fiduciario, il quale provvederà all'inserimento della password.
- Nei casi in cui sia necessario accedere ai dati personali attraverso il server, rivolgersi all'amministratore di sistema o provvedere, in collaborazione con l'amministratore di sistema stesso, alla creazione di credenziali di autenticazione da utilizzarsi esclusivamente per l'accesso da parte degli addetti alla manutenzione/gestione dei sistemi informatici;
- L'amministratore di sistema ha facoltà, in qualunque momento, di controllare e verificare l'operato degli addetti alla manutenzione;
- Qualora si renda necessario prelevare apparecchiature elettroniche per effettuare attività di ripristino o interventi di manutenzione che comportino il reset di password precedentemente

individuate, la nuova password di accesso sarà comunicata all'incaricato il quale provvederà a cambiarla al termine delle operazioni di manutenzione;

- l'accesso al sistema informatico da parte degli addetti alla manutenzione/gestione del sistema è consentito unicamente previo inserimento di password e ID;
- È assolutamente vietato comunicare o diffondere i dati personali di qualsiasi natura provenienti dai database gestiti dell'Istituto, se non previa espressa comunicazione scritta;
- Nel caso in cui ci si avvalga di soggetti esterni per interventi specialistici che comportino trattamento di dati personali deve essere rilasciata una dichiarazione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni in materia di misure minime di sicurezza.

Il Dirigente Scolastico
prof.ssa Maristella Spezzano
Firma autografa sostituita a mezzo stampa ex art.3, c.2 D.Lgs n.39/93