MINISTERO DELL'ISTRUZIONE E DEL MERITO
UFFICIO SCOLASTICO REGIONALE PER IL LAZIO
I S T I T U T O C O M P R E N S I V O "PIO FEDI"
01026 GROTTE S. STEFANO (VT)
(Scuola dell'infanzia, Primaria e Secondaria di 1° grado)
Via Puglia, 25 – tel./ 0761/367026
C.F. 90056690564 – C.U. UF1V31 – Conto di tesoreria unica: 0318092
C.M. VTIC80800L – Codice IPA: istsc_vtic80800l
e mail: vtic80800l@istruzione.it - vtic80800l@pec.istruzione.it
www.piofedi.edu.it

Poiché l'attività istituzionale in cui sono impegnati i

COLLABORATORI SCOLASTICI

implica il trattamento di dati da considerarsi personali, agli effetti della vigente normativa contenuta nel D.Lgs. n.196/2003 e ss.mm. e nel Reg. UE 2016/679;

PRESO ATTO CHE

- il Titolare del Trattamento dei dati personali è l'Istituzione Scolastica legalmente rappresentata dal Dirigente Scolastico;
- il Responsabile per la Protezione dei Dati è il Dott. Pier Giorgio Galli, e-mail pggalli@gallilab.it, tel. 3282878242.

RICHIAMATA

la definizione di trattamento: "qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione", con il presente atto il sottoscritto nella qualità di legale rappresentante del Titolare del trattamento dei dati

AUTORIZZA AL TRATTAMENTO DEI DATI PERSONALI

i **collaboratori scolastici** nei limiti delle operazioni di trattamento e delle categorie di dati personali necessari per l'espletamento delle loro specifiche funzioni, nella misura e nei limiti previsti dalle mansioni assegnate, dagli ordini di servizio ricevuti e dalle istruzioni ivi contenute.
A tal fine si impartiscono le seguenti

ISTRUZIONI[1]

Il trattamento dei dati personali può iniziare solo dopo che l'autorizzato ha ricevuto una formazione adeguata sulla protezione dei dati personali.
La formazione può essere acquisita:

1. partecipando a sessioni di formazione condotte dal Responsabile della protezione dei dati o da un'agenzia approvata dal Titolare del trattamento;
2. seguendo un percorso documentato di autoformazione basato sui contenuti del materiale fornito dal Titolare del trattamento o da altre agenzie approvate dallo stesso e dimostrando di aver compreso appieno i contenuti presentati.

I dati personali che possono essere trattati sono:

- tutti i dati personali di tutti i soggetti con i quali l'Istituzione Scolastica entra in relazione per i suoi fini istituzionali, compresi i dati relativi alla salute e alle altre categorie particolari di dati[2], nella misura e nei limiti previsti dalle mansioni assegnate, dagli ordini di servizio ricevuti e dalle istruzioni ivi contenute.

I dati personali oggetto del trattamento devono essere:

- trattati in modo lecito, corretto e trasparente;
- raccolti solo per gli scopi strettamente necessari alla funzione propria e per finalità determinate, esplicite e legittime;
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per cui sono trattati;
- esatti e, se necessario, aggiornati;
- conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati;
- trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate;

[1] Artt. 29, 32 p.4, RGDP 2016/79; art. 2-quaterdecies, D.Lgs 196/2003.
[2] Art. 9, RGDP 2016/79

- trattati al di fuori della vista di terzi non autorizzati;
- mai comunicati o diffusi a persone non autorizzate al trattamento.

L'autorizzato dovrà inoltre:

- riporre in sicurezza eventuali documenti contenenti dati personali lasciati da altri incustoditi dandone successiva notizia al Titolare del trattamento;

TRATTAMENTO DEI DATI PERSONALI SU SUPPORTO CARTACEO

1. Il trattamento dei dati può avvenire solo all'interno dei locali dell'Istituzione Scolastica;
2. i documenti contenenti dati personali mai devono essere lasciati incustoditi, al termine del trattamento i documenti vanno distrutti o chiusi a chiave in cassetti/armadi muniti di serratura, mai le chiavi dei cassetti/armadi devono essere lasciate incustodite;
3. durante il trattamento dei dati personali su supporto cartaceo vanno poste in atto tutte le misure necessarie per nascondere i dati dalla vista di terzi non autorizzati;
4. i dati personali su supporto cartaceo che, direttamente o indirettamente, possono rivelare lo stato di salute degli interessati possono essere trattati a condizione che siano stati preventivamente anonimizzati o pseudonimizzati;
5. durante le operazioni di fotoriproduzione o stampa occorre assicurarsi che il numero delle copie ottenute siano coincidenti con le copie richieste onde evitare che l'operatore successivo possa raccogliere documenti di cui non è autorizzato al trattamento;
6. è fatto divieto trasferire i dati personali al di fuori della sede scolastica anche temporaneamente. È fatta deroga per quanto attiene le eventuali operazioni di trasferimenti di documenti tra le varie sedi dell'Istituzione Scolastica.

TRATTAMENTO DEI DATI PERSONALI IN FORMA DIGITALE

Misure minime di sicurezza per la gestione e la custodia delle credenziali di autenticazione

Le credenziali di autenticazione sono:

1. assegnate ad uso esclusivo dal Titolare del Trattamento per l'accesso ai dispositivi;
2. assegnate ad uso esclusivo dal Titolare del Trattamento per l'accesso alle piattaforme on line;
3. attivate in autonomia per l'accesso ai dispositivi personali;

Le credenziali di autenticazione devono essere tali da impedirne l'uso illecito, per questo devono essere poste in atto opportune misure di sicurezza:

1. credenziali biometriche (lettura impronta digitale, ecc.) sono intrinsecamente sicure;
2. credenziali con autenticazione a due fattori (es. PIN trasmesso sullo smartphone dopo la digitazione della password) sono intrinsecamente sicure;
3. credenziali di autenticazione incardinate sull'identità digitale (SPID, CIE, ecc.) sono intrinsecamente sicure
4. credenziali formate da nome utente e password o solo password:
    a. le password vanno rinnovate almeno ogni tre mesi senza riusare password simili alle precedenti;
    b. le password non devono essere rivelate a nessuno, né volontariamente né su richiesta. Solo in situazioni di emergenza inderogabile, la password può essere temporaneamente condivisa con un collega fidato, a condizione che venga immediatamente cambiata una volta terminata l'urgenza.
    c. le password mai vanno memorizzata nel browser o in applicazioni analoghe;
    d. le password devono essere mantenute segrete, e qualsiasi supporto cartaceo o digitale su cui siano annotate non deve mai essere lasciato incustodito. Prima di inserire la password, è necessario assicurarsi che nessuno possa vederla durante la digitazione;
    e. le password devono essere composte da almeno 8 caratteri e includere elementi di complessità, come almeno una lettera maiuscola, una lettera minuscola, un numero e un carattere speciale. Non devono contenere parti del nome, data di nascita o nomi di familiari, né porzioni di essi.

Misure minime di sicurezza per il trattamento dei dati in formato digitale

1. L'accesso ai dispositivi digitali che contengono dati personali nelle loro memorie locali è consentito esclusivamente previa autenticazione tramite credenziali personali e riservate. Per i dispositivi digitali che non contengono dati personali, è possibile utilizzare credenziali condivise per l'accesso;
2. il trattamento dei dati personali su piattaforme on line può avere inizio solo dopo la fornitura delle proprie credenziali di autenticazione ad uso esclusivo;
3. il trattamento dei dati personali può avere inizio solo dopo aver verificato che l'antivirus e il firewall siano aggiornati e operativi;
4. il trattamento dei dati personali può avere inizio solo se il sistema operativo e gli applicativi sono aggiornati ovvero gli aggiornamenti vanno installati tempestivamente al ricevimento della notifica;
5. durante il trattamento vanno posti in atto in atto tutti gli accorgimenti tali da nascondere i dati alla vista di terzi non autorizzati;
6. è fatto divieto di consentire ad altri il trattamento dei dati dopo aver avviato il trattamento con le proprie credenziali di autenticazione;
7. al termine del trattamento o in caso di allontanamento temporaneo deve essere eseguita l'operazione di logout in modo che la ripresa del trattamento richieda di nuovo l'autenticazione attraverso la fornitura delle credenziali;
8. la memorizzazione dei dati personali nelle memorie locali dei dispositivi dell'Istituzione scolastica ad uso collettivo (ad esempio, computer delle aule e dei laboratori) non è mai consentita;
9. i documenti contenenti dati personali possono essere memorizzati nelle memorie dei dispositivi di propria pertinenza solo in cartelle non accessibili da altri utenti del medesimo dispositivo;

10. i documenti contenenti dati personali possono essere memorizzati nelle cartelle condivise sulla rete locale o in servizi cloud solo se tali cartelle sono protette da credenziali di autenticazione conformi alle prescrizioni indicate;
11. l'uso di chiavette USB o dispositivi simili per la conservazione dei dati personali è consentito, anche al di fuori dell'Istituzione Scolastica. In tal caso, è necessario garantire che il dispositivo sia fisicamente assicurato a un bene personale, come ad esempio le chiavi di casa, in modo che la sua eventuale perdita venga segnalata tempestivamente;
12. i documenti che, direttamente o indirettamente, possono rivelare lo stato di salute degli interessati possono essere memorizzati nelle memorie locali, di rete o nel cloud solo a condizione che:
    a. siano stati preventivamente anonimizzati o pseudonimizzati;
    b. siano criptati e protetti da una password conforme alle prescrizioni precedentemente indicate.
13. i dati personali che possono rivelare, anche indirettamente, lo stato di salute o che rientrano nelle categorie particolari di dati personali possono essere caricati nei sistemi informativi di agenzie esterne solo previa autorizzazione del Titolare del trattamento.
14. la trasmissione di dati personali via posta elettronica è consentita solo utilizzando caselle di posta elettronica ministeriali o, in alternativa, caselle di posta ufficiali fornite dall'Istituzione Scolastica;
15. l'utilizzo di ambienti cloud per il trattamento dei dati personali è consentito solo se l'Istituzione scolastica ha stipulato un contratto di licenza d'uso con il fornitore (es. registro elettronico);

Nel caso in cui l'autorizzato venga a conoscenza di una violazione dei dati personali che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati, deve darne tempestiva notizia al Titolare del Trattamento o al Responsabile della protezione dei dati.

L'autorizzato è tenuto a segnalare al Titolare o al Responsabile della protezione dei dati eventuali circostanze che rendano necessario o opportuno l'aggiornamento della presente autorizzazione al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

La presente autorizzazione è a tempo indeterminato e si intende automaticamente revocata alla data di cessazione del rapporto attualmente in essere con questa Istituzione scolastica.

Grotte S. Stefano 13/09/2024

Il Dirigente Scolastico
Dott.ssa DIANA Giovanna