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 è impegnato il

DIRETTORE DEI SERVIZI GENERALI E AMMINISTRATIVI (DSGA)

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

il **Direttore Dei Servizi Generali e Amministrativi (DSGA)** nei limiti delle operazioni di trattamento e delle categorie di dati personali necessari per l'espletamento della sua specifica funzione.
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:

1. tutti i dati personali, compresi i dati relativi alla salute e alle altre categorie particolari di dati[2], di cui l'Istituzione Scolastica è titolare.

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;

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

- 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;
- trattati al di fuori della vista di terzi non autorizzati;
- mai comunicati o diffusi a persone non autorizzate al trattamento;
- custoditi e conservati con la diligenza del buon padre di famiglia.

TRATTAMENTO DEI DATI PERSONALI SU SUPPORTO CARTACEO

I dati su supporti cartacei o assimilabili devono trattati nel rispetto delle seguenti prescrizioni:

1. i locali dove sono trattati a qualsiasi titolo documenti cartacei contenenti dati personali devono essere o presidiati da almeno una persona autorizzata o chiusi a chiave;
2. solo l'utenza autorizzata può essere ammessa ai locali dove si trattano o si conservano dati personali su supporto cartaceo;
3. al di fuori dei locali degli uffici amministrativi i documenti cartacei possono essere conservati sono in armadi chiusi a chiave;
4. al di fuori dei locali degli uffici amministrativi i documenti cartacei contenenti dati personali mai vanno lasciati incustoditi;
5. al di fuori dei locali degli uffici amministrativi, 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;
6. i documenti che possono rivelare anche indirettamente lo stato di salute o comunque rientranti nelle categorie particolari dei dati devono essere custoditi in robusti armadi, preferibilmente di metallo, chiusi a chiave presso la sede centrale della scuola. È fatto esplicito divieto conservare nei plessi i dati personali che possono rivelare anche indirettamente lo stato di salute;
7. le copie di documenti che possono rivelare anche indirettamente lo stato di salute o comunque rientranti nelle categorie particolari dei personali vanno pseudonimizzate o anonimizzate. Eccezionalmente è possibile produrre copie con i dati personali in chiaro dell'interessato, o riconducibili all'interessato, solo previa autorizzazione del Titolare del trattamento;
8. 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;
9. è fatto divieto trasferire i dati personali al di fuori delle sedi scolastica anche temporaneamente. È fatta deroga per quanto attiene le eventuali operazioni di trasferimento degli archivi.

TRATTAMENTO DEI DATI PERSONALI IN FORMATO DIGITALE

Misure per l'accesso ai locali dove si svolge il trattamento dei dati personali in formato digitale

1. i locali dove sono trattati i dati personali con dispositivi digitali devono essere presidiati da almeno una persona autorizzata o chiusi a chiave;

Misure 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 per il trattamento dei dati personali con dispositivi digitali

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. almeno con cadenza quadrimestrale va verificata la presenza di software non autorizzato visualizzando l'elenco del software installato con l'apposita funzionalità del sistema operativo;
5. il trattamento dei dati personali può iniziare solo se il sistema operativo e i software applicativi sono aggiornati; gli aggiornamenti devono essere installati tempestivamente al ricevimento della notifica;
6. durante il trattamento vanno posti in atto in atto tutti gli accorgimenti tali da nascondere i dati alla vista di terzi non autorizzati;
7. è fatto divieto di consentire ad altri il trattamento dei dati dopo aver avviato il trattamento con le proprie credenziali di autenticazione;
8. in caso di assistenza remota da parte di agenzie esterne le operazioni compiute da remoto vanno presidiate;
9. 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;
10. 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;
11. 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;
12. i documenti contenenti dati personali possono essere memorizzati in memorie removibili come ad esempio dischi esterni. In questo caso le memorie, quando non in uso, vanno custodite in un luogo sicuro all'interno dell'Istituzione Scolastica;
13. 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;
14. i documenti digitali che possono rivelare, anche indirettamente, lo stato di salute o che rientrano nelle categorie particolari di dati personali devono essere conservati esclusivamente nel sistema di gestione documentale scolastico. In via eccezionale, qualora sia necessario memorizzare tali documenti in altre memorie locali, di rete o cloud, essi devono essere criptati e protetti da una password conforme alle prescrizioni precedentemente indicate;
15. 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.
16. i dati personali che possono rivelare, anche indirettamente, lo stato di salute o che rientrano nelle categorie particolari di dati personali possono essere trasmessi per posta elettronica solo se allegati criptati e previa autorizzazione del Titolare del trattamento. La chiave di decriptazione deve essere inviata separatamente, preferibilmente tramite un mezzo di comunicazione diverso;
17. è obbligatorio effettuare un backup settimanale dei dati archiviati nelle memorie dei dispositivi di propria pertinenza, la cui perdita, in caso di disastro, potrebbe compromettere il corretto svolgimento delle future procedure amministrative;
18. 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;
19. 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. sistema di gestione documentale).

PUBBLICAZIONE DI CONTENUTI NEL SITO WEB ISTITUZIONALE O IN PIATTAFORME SOCIAL UFFICIALI

Premesso che la pubblicazione di dati personali sul sito web istituzionale o sui social ufficiali della scuola può avvenire esclusivamente per perseguire finalità didattiche o per promuovere l'offerta formativa della scuola, si precisa che:

- non possono essere pubblicati dati personali che rivelino categorie particolari, come l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, dati genetici, biometrici (intesi a identificare in modo univoco una persona), o dati relativi alla salute, alla vita sessuale o all'orientamento sessuale della persona. Inoltre, non devono essere divulgati dati relativi a condanne penali o reati;
- i contenuti pubblicati devono limitarsi ai dati personali strettamente necessari per raggiungere le finalità del trattamento;
- i dati personali devono rimanere in pubblicazione solo per il periodo minimo previsto dalla legge o dai regolamenti applicabili;
- la pubblicazione di dati personali è consentita solo previa autorizzazione del Titolare del trattamento e dopo aver acquisito le eventuali liberatorie necessarie.

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