Ministero dell'Istruzione e del Merito
Ufficio Scolastico Regionale per il Lazio
ISTITUTO OMNICOMPRENSIVO "LEONARDO DA VINCI" ACQUAPENDENTE
Via G. CARDUCCI s.n.c. 01021 Acquapendente (VT) CF 80019550567 – Tel. 0763/734208
e-mail vtis01100l@istruzione.it; PEC: vtis01100l@pec.istruzione.it
CODICE UNIVOCO: UFKJ4I

Poiché l'attività istituzionale in cui sono impegnati i

DOCENTI

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 della 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 **Docenti** nei limiti delle operazioni di trattamento e delle categorie di dati necessari ai fini dello svolgimento della funzione propria.
A tal fine si impartiscono le seguenti

ISTRUZIONI

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, inclusi quelli relativi alla salute e ad altre categorie particolari, riguardanti gli studenti, i genitori e altri interessati quando ciò è necessario per l'esecuzione delle attività didattiche svolte dal docente o per altri incarichi a lui affidati.

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;
- trattati al di fuori della vista di terzi non autorizzati;
- mai comunicati o diffusi al di fuori del Titolare del trattamento, della classe di pertinenza, dei membri degli organi collegiali competenti, dei genitori o di chi altri eserciti la responsabilità genitoriale;
- custoditi e conservati con la diligenza del buon padre di famiglia.

TRATTAMENTO DEI DATI PERSONALI SU SUPPORTO CARTACEO

1. Il trattamento dei dati può avvenire solo all'interno dei locali dell'Istituzione Scolastica, è fatta deroga per quanto attiene alle operazioni relative alla correzione degli elaborati scritti/grafici purché siano poste in atto adeguate misure tecniche si sicurezza (es. pseudonimizzazione) atte ad impedire la riconducibilità dei dati personali (es. voti, giudizi) all'identità degli studenti;
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. i documenti contenenti dati personali vanno distrutti al termine del progetto didattico fatta eccezione per gli elaborati scritti da consegnare entro il termine dell'anno al personale preposto per le operazioni di archiviazione.

TRATTAMENTO DEI DATI PERSONALI IN FORMA DIGITALE

Misure minime di sicurezza per l'accesso al registro elettronico.

L'accesso al registro elettronico **deve avvenire esclusivamente mediante l'utilizzo di identità digitali (CIE, SPID, ecc.)**. Si distinguono i seguenti casi:

1. Il registro elettronico consente l'accesso esclusivamente con identità digitale:
   1.1. accedere fornendo la propria identità digitale.
2. Il registro elettronico consente l'accesso sia tramite identità digitale sia tramite credenziali tradizionali:
   2.1. impostare la password con una sequenza casuale di almeno 14 caratteri, comprendente lettere maiuscole, lettere minuscole, numeri e caratteri speciali (es. *TfGr12aC?@df67*), la password non deve essere conservata né annotata. **Tale prescrizione comporta che la password venga inevitabilmente dimenticata e, di conseguenza, resa inutilizzabile**;
   2.2. accedere fornendo la propria identità digitale.
3. Il registro elettronico non consente l'accesso tramite identità digitale:
   3.1. accedere fornendo nome utente e password.

Misure minime di sicurezza per l'accesso alle piattaforme didattiche.

Premesso che sono utilizzabili solo le piattaforme didattiche per le quali è in essere un contratto tra la scuola e il fornitore (es. Google Classroom, Microsoft Teams, ecc.), l'accesso a tali piattaforme **deve avvenire esclusivamente mediante l'autenticazione a due fattori (2FA). Solo nel caso in cui l'autenticazione a due fattori non fosse disponibile è ammesso l'accesso con il nome utente e password.**

Misure minime di sicurezza per le password.

Le password devono rispettare i seguenti requisiti minimi di sicurezza:

1. essere composte da almeno 8 caratteri (14 nel caso di utenze amministrative) e includere elementi di complessità: 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, ecc., né porzioni di essi;
2. essere rinnovate almeno ogni tre mesi senza riusare password simili alle precedenti;
3. non 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;
4. non essere mai vanno memorizzata nel browser o in applicazioni analoghe.

È possibile annotare le password su supporto cartaceo solo adottando adeguati sistemi di cifratura.
È possibile memorizzare le password su file protetto da cifratura.

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;
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. in caso di assistenza remota da parte di agenzie esterne le operazioni compiute da remoto vanno presidiate;
8. 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;
9. 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;
10. i documenti contenenti dati personali possono essere memorizzati nelle memorie dei dispositivi di proprietà dell'autorizzato solo in cartelle a cui non abbiano accesso altri utenti dello stesso 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. 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;
13. 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.
14. 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.
15. 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;
16. 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;
17. 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 (ad esempio, per il registro elettronico);
18. prima di consentire agli studenti l'accesso a un ambiente didattico basato su cloud, è fondamentale verificare le loro competenze in materia di sicurezza informatica, privacy e cyberbullismo, colmando eventuali lacune. Le azioni intraprese per migliorare queste competenze devono essere documentate nel registro di classe;
19. al termine del progetto didattico, i documenti digitali contenenti i dati personali degli studenti devono essere eliminati. Allo stesso modo, devono essere rimossi anche i dati personali caricati negli ambienti didattici online;
20. in occasione di colloqui e/o riunioni a distanza, è necessario verificare che siano presenti e in ascolto esclusivamente persone autorizzate al trattamento dei dati.

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 ha validità a tempo indeterminato, sostituisce ogni eventuale precedente ed è automaticamente revocata alla cessazione del rapporto di lavoro con la presente Istituzione scolastica.

Acquapendente 12/09/2025

IL DIRIGENTE SCOLASTICO
(Dott.ssa Luciana BILLI)
Documento firmato digitalmente ai sensi del c.d.
Codice dell’ Amministrazione Digitale e normativa connessa