Istituto di Istruzione Superiore

"G. COLASANTI " di Civita Castellana (VT)

Liceo Classico, Liceo Scientifico– Istituto Tecnico Economico

Istituto Professionale Odontotecnico - Serale

Sede Uffici di Dirigenza e Segreteria: Via F. Petrarca snc – 01033 Civita Castellana (VT)

Tel. 0761/513394-515720 – sede di via Berlinguer: tel. 0761/515143

e-mail: vtis006005@istruzione.it; pec vtis006005@pec.istruzione.it

sito: www.iiscolasanti.edu.it - - C.F. 90056780563

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 Scolasticastessa legalmente rappresentata dal Dirigente Scolastico;
- il Responsabile per la Protezione dei Datiè 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 Dirigente Scolastico nella qualità di legale rappresentante pro tempore del Titolare del trattamento dei dati

AUTORIZZA AL TRATTAMENTODEI DATI

i **docenti**nei limiti delle operazioni di trattamento e delle categorie di dati necessari ai fini dello svolgimento della funzione propria, ovvero, relativamente alle categorie particolari di dati personali[1] e ed ai dati relativi a condanne penali e reati[2], quando "il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato**"**[3]**.**
A tal finesi impartiscono le seguenti

ISTRUZIONI[4]

I dati personali degli studenti, raccolti per l'espletamento della funzione docente, sono trattati:

- nel registro personale del docente;
- nel registro di classe;
- nel registro delle evacuazioni;
- nei registri dei verbali;
- nella raccolta degli elaborati scritti o grafici o digitali prodotti dagli studenti;
- negli archivi digitali personali del docente;
- negli ambienti on line di supporto alla didattica digitale.
- nelle comunicazioni scuola/famiglia;
- nella documentazione accessoria per l'organizzazione delle attività didattiche.

I dati personali oggetto del trattamento devono essere:

- trattati in modo lecito, corretto e trasparente;
- raccolti solo per gli scopi strettamente necessari alla funzione docente e per finalità determinate, esplicite e legittime;

[1] Art. 9, RGDP 2016/79.
[2] Art. 10, RGDP 2016/79.
[3] Art.9, par.2, lett. g, RGDP 2016/79.
[4] Artt.29, 32 p.4, RGDP 2016/79; art. 2-quaterdecies, D.Lgs 196/2003.

- 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 Dirigente Scolastico, della classe di pertinenza, dei componenti degli organi collegiali di pertinenza,dei genitori degli studenti o di chi ne fa le veci;
- 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 delle adeguate tecniche di pseudonimizzazione;
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. i documenti contenenti dati personali vanno distrutti al termine del progetto didattico fatta eccezione per gli elaborati scrittida 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 la gestione e la custodia delle credenziali di autenticazione

Le credenziali di autenticazione sono:

1. assegnate ad uso esclusivo dall'Istituzione Scolastica per l'accesso ai dispositivi;
2. assegnate ad uso esclusivo dall'Istituzione Scolastica per l'accesso ai servizi cloud;
3. attivate in autonomia per l'accesso ai dispositivi personali;
4. attivate in autonomia per l'accesso ai servizi cloud personali;

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

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 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 passwordnon devono essere rivelate né di propria iniziativa né dietro richiesta, ad alcuno. Solo in caso di urgenze indifferibili la password può essere comunicata ad un collega fidato per essere rinnovata tempestivamente terminata l'urgenza;
    c. le passwordmai vanno memorizzata nel browser o in applicazioni analoghe;
    d. le passwordvanno mantenute segrete, mai dovranno essere lasciati incustoditi gli eventuali supporti cartacei o digitali dove è stata annotata. Prima di digitare la password occorre verificare che nessuno possa prenderne visione durante la digitazione;
    e. le passworddevono contenere almeno 8 caratteri (14 caratteri per utenze amministrative) con elementi di complessità (almeno un carattere maiuscolo, uno minuscolo, un numero, un carattere speciale) enon deve contenere parti del nome né la sua data di nascita o parte di essa né nomi o parte di nomi dei famigliari, ecc.;
4. credenziali formate da nome utente e gestureo solo gesture:
    a. le gesture vanno rinnovate almeno ogni tre mesi;
    b. le gesture devono contenere elementi di complessità;

Misure minime per la memorizzazione di dati personali che possono rivelare anche indirettamente lo stato di salute

1. I documenti digitali che possono rivelare anche indirettamente lo stato di salutedelle persone possono essere conservati in chiaro solo nel sistema di gestione documentale scolastico. Nel caso in cui si renda necessario, per motivi operativi, memorizzare i documenti su memorie diverse (es. desktop, chiavette, ecc.) o si renda necessario trasmettere tali documenti per posta elettronica o con altro mezzo, allora i documenti vanno protetti con password di almeno 8 caratteri con complessità (almeno un carattere maiuscolo, uno minuscolo, un carattere numerico e un simbolo speciale).

Misure minime di sicurezzaper il trattamento dei dati personali con i dispositivi della scuola (es. notebook delle cattedre)

1. Il trattamento dei dati può avere inizio solo dopo aver verificato che l'antivirus sia aggiornato e operativo;
2. durante il trattamento occorre porre in atto tutti gli accorgimenti tali da nascondere i dati alla vista di terzi non autorizzati;
3. è fatto divieto di consentire ad altri il trattamento dei dati dopo aver avviato il trattamento con le proprie credenziali di autenticazione;
4. il sistema operativo e gli applicativi vanno aggiornati tempestivamente al ricevimento della notifica.

5. 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.
6. **la conservazione dei dati personali nelle memorie dei dispositivi della scuola mai è ammesso**. Al termine del trattamento dei dati personali i documenti vanno cancellati e subito eliminati dal cestino;
7. **nel caso in cui vengano scaricati degli allegati dalla casella di posta personale**gli allegati vanno al termine cancellati dalla cartella download e subito eliminati dal cestino.

Misure minime di sicurezzaper il trattamento dei dati personali con dispositivi di proprietà del personale (compresi gli eventuali dispositivi della scuola affidati ad uso esclusivo)

1. punti da 1 a 5 della sezione precedente "Misure minime di sicurezza per il trattamento dei dati personali con i dispositivi della scuola"
2. la scansione completa antivirus va effettuata almeno ogni 30 giorni;
3. lo stato di funzionalità del firewall va fatto almeno ogni almeno ogni 30 giorni;
4. la memorizzazione dei dati può avvenire solo sul desktop o nella cartella documenti (o comunque in aree di memoria non accessibili agli altri utenti del computer).

Misure minime di sicurezza per il trattamento dei dati personali conservati nelle chiavette USB

L'uso di chiavette USB per la conservazione dei dati personali è ammessa solo sela memoria rimovibile è fisicamente assicurata ad un bene personalela cui eventuale perdita deve essere accertata per impostazione predefinita entro il termine della giornata (es. chiavetta USB solidamente assicurata alla chiave di casa o dell'automobile e mai da queste separate neanche durante l'uso).

Misure minime di sicurezza per il trattamento dei dati personali su piattaforme cloud

L'accesso alle piattaforme cloud può avvenire utilizzando sia i dispositivi della scuola sia i dispositivi personali nel rispetto delle seguenti misure minime di sicurezza:

1. gli ambienti didatticicloud utilizzabili sono elencati nel Piano Scolastico per la Didattica Digitale Integrata o comunque autorizzati dal Dirigente Scolastico sentito il responsabile della protezione dei dati;
2. i dati personali vanno cancellati al termine del progetto didatticodopo aver scaricato gli elaborati degli studenti a valere per gli scrutini per il successivo versamento nell'apposito repository a ciò dedicato dall'Istituzione Scolastica;
3. il docente prima di utilizzare la piattaformaverifica l'adeguatezza delle competenze degli studenti in tema di sicurezza informatica, privacy e cyberbullismo integrandone le eventuali carenze. Le eventuali azioni poste in atto per adeguare le competenze degli studenti vanno annotate nel registro di classe;

Misure minime di sicurezza per la trasmissione di dati personali

1. la trasmissione di dati personali tra il personale dipendente e l'Istituzione Scolastica o tra il personale e l'utenza può avvenire solo tramite la posta elettronica istituzionale (fornita dal ministero o dalla scuola) o attraverso il registro elettronico;
2. è vietato l'uso di piattaforme social per la comunicazione di dati personali.

PUBBLICAZIONE DI CONTENUTI NEL SITO WEB ISTITUZIONALE

I docenti autorizzati alla pubblicazione di contenuti nel sito web istituzionalediffondono documenti contenenti dati personali solo dopo aver accertato il fondamento normativo (legge o regolamento) che obbliga o autorizza l'Istituzione Scolastica alla pubblicazione dei dati o, in alternativa, a seguito di disposizioni specifiche impartite dal Titolare.

In ogni caso i documenti pubblicati:

1. mai devono contenere categorie particolari di dati personali[5] che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, datibiometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;
2. mai devono contenere dati personali relativi a condanne penali e reati[6];
3. devono contenere solo i dati indispensabili;
4. devono rimanere in pubblicazione per il numero minimo dei giorni previsti dalla legge o regolamento.

PER TUTTI I TRATTAMENTI

- Se il trattamento dei dati personali può rivelare, anche indirettamente, lo stato di salute, l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, la vita sessuale o l'orientamento sessuale della persona, allora il nome e cognome dell'interessato (e gli eventuali altri dati identificativi) vanno pseudonimizzati;
- nel caso in cui il dipendente 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;
- il dipendentedeve 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

[5] Art. 9, RGPD 2016/679.
[6] Art. 10, RGPD 2016/679.

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.

Civita Castellana 01/09/2023

Il Dirigente Scolastico
Prof.ssa Angela De Angelis
Documento firmato digitalmente