



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

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 Scolasticastessa 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 Dirigente Scolastico nella qualità di legale rappresentante pro tempore del Titolare del trattamento dei dati

AUTORIZZA AL TRATTAMENTO DEI DATI

i **collaboratori scolastici** 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 personali¹ e ed ai dati relativi a condanne penali e reati², 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 fine si impartiscono le seguenti

ISTRUZIONI⁴

Il **collaboratore scolastico** è autorizzato il trattamento dei 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 dalle mansioni assegnate, dagli ordini di servizio ricevuti e dalle istruzioni ivi contenute.

Specificamente il trattamento è autorizzato in occasione di:

- comunicazioni telefoniche;
- identificazione dei visitatori;
- duplicazione attraverso fotocopie;
- trasporto e consegna di documenti;

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.

- affissione di documenti nelle bacheche;
- archiviazione di documenti.

I dati personali oggetto del trattamento devono essere:

- trattati in modo lecito, corretto e trasparente;
- raccolti solo per gli scopi strettamente necessari alla funzione propriae 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 a persone non autorizzate al trattamento;
- custoditi e conservati con la diligenza del buon padre di famiglia.

Il collaboratore scolastico dovrà:

- procedere al trattamento dei dati personali secondo gli ordini di servizio e le istruzioni ricevute;
- nascondere alla vista di persone non autorizzate i documenti contenenti dati personali;
- rispettare il divieto assoluto di divulgazione in qualunque forma o modalità, analogica o digitale, dei dati trattati;
- raccogliere e conservare per il tempo strettamente necessario le generalità dei visitatori che si recano presso le sedi dell'Istituto Scolastico, comunicandoli a chi di competenza per l'espletamento delle operazioni richieste;
- segnalare al titolare o al Responsabile Della Protezione dei Dati eventuali circostanze che rendano necessario od opportuno l'aggiornamento delle predette istruzioni 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;
- comunicare, diffondere o trasferire all'esterno i dati personali esclusivamente ai soggetti autorizzati (previa identificazione) nel rispetto delle istruzioni ricevute;
- mantenere la massima riservatezza sui dati personali dei quali si venga a conoscenza nello svolgimento dell'incarico, per tutta la durata del medesimo ed anche successivamente al termine di esso;
- prestare la più ampia e completa collaborazione al titolare al fine di compiere tutto quanto sia necessario ed opportuno per il corretto espletamento dell'incarico nel rispetto della normativa vigente;
- chiudere gli eventuali cassetti contenenti dati personali lasciati aperti dai docenti e darne notizia al DS;
- spegnere i computer eventualmente lasciati accesi e darne notizia al DS;
- raccogliere e riporre in cassetti chiusi a chiave eventuali documenti contenenti dati personali lasciati incustoditi e darne notizia al DS;

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 password non 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 password mai vanno memorizzate nel browser o in applicazioni analoghe;
 - d. le password vanno 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 password devono contenere almeno 8 caratteri (14 caratteri per utenze amministrative) con elementi di complessità (almeno un carattere maiuscolo, uno minuscolo, un numero, un carattere speciale) e non 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 gestore solo gestore:
 - a. le gestore vanno rinnovate almeno ogni tre mesi;
 - b. le gestore devono contenere elementi di complessità;

Misure minime di sicurezza per 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 computer (es. desktop), tablet o altri dispositivi 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,** al termine gli allegati vanno cancellati dalla cartella download e subito eliminati dal cestino.

Misure minime di sicurezza per il trattamento dei dati personali con dispositivi propri (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 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 se la memoria rimovibile è fisicamente assicurata ad un bene personale la 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 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.

PER TUTTI I TRATTAMENTI

- 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 dipendente deve 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.

Civita Castellana, 11/09/2023

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