REPUBBLICA ITALIANA

PROVINCIA AUTONOMA DI TRENTO

ISTITUTO COMPRENSIVO ALDENO-MATTARELLO
Via della Torre Franca, 1 - 38060 MATTARELLO – (Trento)
Tel. 0461/945237 - Fax. 0461/946007 C.F. 96056860222 - e-mail: segr.aldeno.mattarello@scuole.provincia.tn.it

Mattarello-Trento,

Mattarello, 30 settembre 2019
Prot. 783274.1

A tutto il personale docente e non docente
IC Aldeno-Mattarello

OGGETTO: VADEMECUM SUL TRATTAMENTO DEI DATI (PRIVACY)

Tutto il personale è tenuto a conoscere e a osservare la normativa sulla privacy. Al fine di assicurare agli Interessati (alunni, genitori, fornitori di beni e servizi, il personale stesso, ecc) un trattamento dei dati lecito dei propri dati e garantito da adeguate misure di sicurezza, si comunicano le seguenti misure operative cui tutto il personale dovrà scrupolosamente attenersi, oltre a quanto indicato nella lettera di incarico e nel Registro dei trattamenti.

Si ricorda che per trattamento dati personali si intende la loro raccolta, registrazione, organizzazione, conservazione, elaborazione, modifica, selezione, estrazione, raffronto, utilizzo, interconnessione, blocco, comunicazione, diffusione, cancellazione e distruzione, svolte con o senza l'ausilio di mezzi elettronici.

RACCOLTA DEI DATI:

- Prima di procedere alla raccolta e al trattamento dei dati fornire sempre l'informativa all'interessato, consegnando, quando necessario, il modulo per il consenso (es. informativa per l'uso della G Suite, per le immagini, per i viaggi di istruzione, ecc.). A titolo puramente esemplificativo e non esaustivo viene raccolto ad esempio il nome ed il cognome, l'indirizzo di posta elettronica (e-mail), l'indirizzo, un recapito postale o altre informazioni necessarie per contattare l'utente e per lo svolgimento dei vari servizi che vengono forniti dall'Istituto.
- Accedere solo ai dati strettamente necessari all'esercizio delle proprie mansioni e conservarli per il periodo di tempo necessario agli scopi per i quali essi sono stati raccolti.

TRATTAMENTO DEI DATI IN GENERALE

- Verificare che i dati siano esatti e, se necessario, aggiornarli.
- Controllare e custodire gli atti e i documenti contenenti dati personali in modo da assicurarne l'integrità e la riservatezza.
- Non comunicare a terzi qualsiasi dato personale, al di fuori dell'ambito lavorativo, o in difformità dalle istruzioni ricevute.
- Non fornire telefonicamente o a mezzo elettronico dati e informazioni relativi a terzi, senza una specifica autorizzazione del Titolare (Dirigente Scolastico) e, comunque, senza avere la certezza della loro identità; qualora giungano richieste telefoniche di dati sensibili da parte dell'Autorità Giudiziaria o degli organi di polizia si deve richiedere l'identità dell'interlocutore. Quindi si provvederà a richiamare, avendo così la certezza sull'identità del richiedente.
- Gli insegnanti possono diffondere i dati degli alunni (nomi, foto e video) solo dopo avere richiesto ed ottenuto la relativa autorizzazione scritta di chi esercita la patria podestà che si dovrà riferire unicamente a quella specifica situazione, evento o progetto. In ogni caso si dovrà applicare il principio della minimizzazione del trattamento, ovvero dell'uso strettamente necessario, ad esempio del nome e cognome per esteso in luogo delle iniziali e del volto

identificabile dell'alunno piuttosto che di una foto dello stesso non in primo piano. In tali casi bisogna valutare se l'identificazione dell'alunno aggiunga effettivo valore documentativo o pedagogico tali da giustificarne la diffusione. Qualora non tutti i genitori abbiamo autorizzato il trattamento dei dati è possibile diffondere solo i dati degli alunni autorizzati (es, foto per il sito web di un eventuale organizzatore di progetto o sponsor senza gli alunni non autorizzati).

- Non lasciare a disposizione di estranei documenti o supporti di memorizzazione (cd, dvd, pen drive) che contengono dati personali e/o particolari.
- Non lasciare incustoditi registri o fogli contenenti gli indirizzi ed i recapiti telefonici del personale e dei genitori.
- Accertarsi che al termine delle lezioni o del turno di lavoro, o comunque in caso di assenze prolungate dalla postazione di lavoro i computer siano spenti e che i documenti con dati sensibili eventualmente utilizzati siano stati ricollocati negli appositi armadi e chiusi a chiave.
- Effettuare copie fotostatiche di documenti con dati personali o sensibili nel numero limitato allo scopo, usando le fotocopiatrici posizionate nei locali accessibili ai soli addetti ai lavori.
- I documenti cartacei non più utilizzati, contenenti anche solo dati personali, devono essere distrutti o comunque resi illeggibili, prima di essere eliminati o cestinati.
- Per l'accesso al sistema informatico utilizzare le credenziali ricevute e adottare le necessarie cautele per assicurare la segretezza della parola chiave e la diligente custodia di ogni altro dispositivo di autenticazione informatica (badge, schede magnetiche, chiavi USB, etc.). Conservare quindi con cura la password evitando di trascriverla su fogli posti in vista in prossimità del PC o sulla rubrica dell'ufficio. Al termine di qualsiasi lavoro a un terminale o dispositivo digitale, ricordarsi di effettuare la disconnessione dal proprio account.
- E' vietato comunicare a qualunque altro incaricato le proprie credenziali di accesso al sistema informatico.
- Nell'utilizzo della posta elettronica non aprire documenti di cui non sia certa la provenienza, utilizzare l'antivirus.
- Controllare accuratamente l'indirizzo dei destinatari prima di inviare email contenenti in allegato o nel corpo del messaggio dati personali (per le mail collettive usare la funzione di invio CCN, per evitare di evidenziare chi siano gli altri destinatari e quale sia il loro indirizzo di posta elettronica).
- E' vietato utilizzare social network quali Facebook, Whatsapp o altri per la pubblicazione e/o la diffusione di dati inerenti gli studenti o per comunicare con le famiglie.
- I registri personali cartacei vanno sempre conservati negli armadietti provvisti di serratura. Non è consentito l'accesso degli alunni in aula degli insegnanti, neppure se autorizzati dai docenti.
- I collaboratori scolastici e il personale di segreteria sono tenuti a chiudere a chiave la porta di accesso agli uffici durante la pausa pranzo e sempre a conclusione dell'ultimo turno di lavoro di segreteria.

TRATTAMENTO DEI DATI PARTICOLARI O SENSIBILI

- Non inviare via mail messaggi contenenti il nome per esteso di alunni o di qualsiasi persona nei casi di trattamento di dati sensibili (alunni con BES, persone seguite dai servizi sanitari, assistenziali, giudiziari, ecc.), avendo cura di indicarli solo con le iniziali, di non allegare documenti, anche se proveniente da terzi, in cui siano trattati i dati sensibili (ad es. i certificati medici) e di consegnarli al personale di segreteria incaricato o alla dirigente scolastica oppure farli recapitare agli stessi in busta chiusa, mettendo in campo tutte le attenzioni necessarie.
- I docenti autorizzati a trattare i dati sensibili degli alunni possono visualizzare la documentazione chiusa a chiave nell'armadio del locale dedicato riservato agli addetti ai lavori,

dopo avere firmato il registro di accesso allo stesso, in presenza del personale di segreteria. A consultazione conclusa gli stessi docenti sono tenuti a restituire la documentazione al personale di segreteria e a firmare nuovamente il registro per l'avvenuta riconsegna della documentazione.

- Le comunicazioni riguardanti i profili degli alunni vengono trasmesse al personale incaricato (es. commissione di continuità, docente di sostegno, docente tutor) che le divulgherà ai colleghi di classe in modo riservato e solo verbalmente.

DATI INCUSTODITI O SMARRITI

- Segnalare tempestivamente la presenza di documenti incustoditi o di supporti di memorizzazione (cd, dvd, pen drive), provvedendo temporaneamente alla loro custodia e alla chiusura dei locali in cui sono conservati.

L'art 33 del Regolamento UE 2016/679 prevede l'obbligo di notificare al Garante per la protezione dei dati entro 72 ore la "violazione dei dati personali" (data breach), ovvero la distruzione, la modifica o la divulgazione non autorizzata, l'accesso abusivo ai dati e lo smarrimento o il furto di documentazione o di un supporto di memorizzazione contenente dati personali.

Si precisa che il titolare (dirigente scolastico) è sempre e comunque responsabile della mancata esecuzione degli adempimenti previsti dal D.Lgs. n.196/2003 e del Regolamento UE 2016/679. Tuttavia le responsabilità, per l'inosservanza delle istruzioni impartite dal titolare e/o dai responsabili, possono riguardare anche gli incaricati (docenti e personale non docente) che non rispettino o non adottino le misure necessarie.
Si chiede pertanto di porre la massima attenzione nel monitorare e rilevare tempestivamente tutte le potenziali e reali violazioni dei dati e di comunicarli prontamente alla dirigente scolastica. Si ricorda che la tardiva o omessa notificazione al garante di una "violazione dei dati personali" è punita con sanzioni pecuniarie di rilevante entità.

La Dirigente Scolastica
Prof.ssa T. Chiara Pasquini