ISTITUTO COMPRENSIVO I - UDINE
Via Val di Resia, 13 - 33100 UDINE
Tel 0432 470855 - Fax 0432 547719
Email: UDIC84100A@istruzione.it ***Pec***: UDIC84100A@pec.istruzione.it ***Sito:*** 1icudine.gov.it
Codice MIUR UDIC84100A – CF 94127270307

Udine, 20 novembre 2018

Al sito d'Istituto

Oggetto: POLITICA PROTEZIONE DEI DATI PERSONALI

L'Istituto Comprensivo I Udine raccoglie e utilizza determinati dati sulle persone. Questi possono includere *stakeholder* con cui questa Istituzione scolastica ha una relazione o potrebbe aver bisogno di contattare.

La politica contenuta in questo documento descrive come tali dati personali devono essere raccolti, gestiti e archiviati per soddisfare gli standard di protezione dei dati delineati dal Regolamento UE 2016/679 del Parlamento europeo del Consiglio del 27 aprile 2016, nonché dal Codice Privacy di cui al D. Lgs. n. 196 del 2003 come da ultimo novellato con il D. Lgs. 101/2018.

SCOPO

Questa politica di protezione dei dati garantisce che l'Istituzione scolastica:

- operi conformemente alla legge sulla protezione dei dati personale e segua le buone pratiche;
- protegga i diritti di personale, stakeholder e partner;
- sia trasparente su come raccoglie e tratta i dati degli individui;
- si protegga dai rischi di una violazione dei dati personali.

CAMPO Dl APPLICAZIONE

Questa politica si applica ai dipendenti, collaboratori, consulenti, lavoratori temporanei, incluso tutto il personale affiliato a terze parti e a tutte le attrezzature di proprietà o in *leasing* dell'Istituzione scolastica.

MODALITÀ OPERATIVE

Il Regolamento UE 679/2016 (GDPR) descrive come le organizzazioni, incluso l'Istituto Comprensivo I Udine, devono raccogliere, gestire e archiviare i dati personali.

Queste regole si applicano indipendentemente dal fatto che i dati siano archiviati elettronicamente, su carta o su altri materiali.

Per rispettare la legge, le informazioni personali devono essere raccolte e utilizzate correttamente, conservate in modo sicuro e non divulgate illegalmente.

Il GDPR (Regolamento UE 679/2016) è sostenuto da otto importanti principi, linee guida su come trattare il dato personali. In particolare i dati personali devono:

1) Essere trattati in modo equo e legale
2) Essere ottenuti solo per finalità specifiche, lecite
3) Essere adeguati, pertinenti e non eccessivi
4) Essere precisi e aggiornati
5) Non essere trattenuti più a lungo del necessario
6) Essere elaborati conformemente ai diritti degli interessati
7) Essere protetti nei modi appropriati
8) Non essere trasferiti al di fuori dello Spazio economico europeo (SEE), a meno che tale paese o territorio garantisca anche un livello adeguato di protezione, ci sia una base contrattuale o sia state delineate delle BRC (*Binding Corporate Rules*)

APPLICAZIONE, RISCHI E RESPONSABILITÀ

Questa politica si applica all'organizzazione nel suo intero:
- Sede centrale
- Tutti i plessi
- Tutto il personale e i volontari
- Tutti gli appaltatori, i fornitori e le altre persone che operano per conto dell'organizzazione

Si applica a tutti i dati che l'Istituzione scolastica detiene in relazione a persone identificabili. Ciò può includere:

- Nomi di individui
- Indirizzi postali
- Indirizzi e-mail
- Numeri di telefono
- oltre a qualsiasi altra informazione relativa alle persone

RISCHI

Questa politica aiuta a proteggere l'organizzazione da alcuni rischi di sicurezza dei dati personali molto reali, tra cui:
- violazioni di riservatezza (le informazioni personali vengono ottenute, modificate, cancellate o distribuite in modo inappropriato);
- non riuscire a offrire una scelta (tutte le persone dovrebbero essere libere di scegliere in che modo l'organizzazione utilizza i dati che le riguardano);
- danno reputazionale (l'organizzazione potrebbe soffrire un danno d'immagine in caso di *data breach*).

RESPONSABILITÀ

Chiunque lavori per o con l'Istituto Comprensivo I Udine ha la responsabilità di garantire che i dati personali vengano raccolti, archiviati e gestiti in modo appropriato.

Ogni persona che gestisce i dati personali deve garantire che siano gestiti e elaborati in linea con questa politica e i principi di protezione dei dati.

In particolare, le seguenti persone hanno ruoli chiave di responsabilità:

Il Dirigente Scolastico/Titolare di trattamento è in ultima analisi responsabile di garantire che l'organizzazione soddisfi i propri obblighi legali.

Il Responsabile della protezione dei dati (DPO) è responsabile di:

- mantenere il titolare di trattamento aggiornato sulle responsabilità, i rischi e le questioni relativi alla protezione dei dati.
- revisionare tutte le procedure di protezione dei dati e le relative politiche, in linea con un programma concordato.
- organizzare la formazione e la consulenza sulla protezione dei dati per le persone coperte da questa politica.
- gestire le domande sulla protezione dei dati da parte del personale e di chiunque altro coperto da questa politica.
- gestire le richieste da parte di individui per vedere i dati che l'Istituzione scolastica tiene su di loro
- verificare e approvare eventuali contratti o accordi con terze parti che possano gestire i dati personali trattati dall'organizzazione.

L'Amministratore di sistema è responsabile di:

- garantire che tuffi i sistemi, i servizi e le apparecchiature utilizzate per la memorizzazione dei dati soddisfino standard di sicurezza accettabili
- eseguire controlli e scansioni regolari per garantire che l'hardware e il software di sicurezza funzionino correttamente
- valutare eventuali servizi di terzi che l'Istituto sta considerando di utilizzare per archiviare o elaborare dati (ad esempio, servizi di *cloud computing*.)

LINEE GUIDA GENERALI PER IL PERSONALE

Le uniche persone in grado di accedere ai dati coperti da questa politica dovrebbero essere coloro che ne hanno necessità per il loro lavoro.

I dati non devono essere condivisi in modo informale. Quando è richiesto l'accesso ad informazioni confidenziali, i dipendenti si rivolgono al Titolare del Trattamento o a chi ne fa le veci.

L'Istituzione scolastica fornirà formazione a tutti i dipendenti per aiutarli a comprendere le loro responsabilità nella gestione dei dati.

I dipendenti devono mantenere tutti i dati personali al sicuro, adottando precauzioni e seguendo le linee guida presentate in questa politica. In particolare, è necessario:

- utilizzare password complesse, che non devono mai essere condivise.
- i dati personali non devono essere divulgati a persone non autorizzate, all'interno dell'organizzazione o esternamente
- i dati personali devono essere rivisti e regolarmente aggiornati. Se non sono più necessari, devono essere eliminati

- i dipendenti, prima di agire, devono chiedere supporto al Titolare del Trattamento se non sono sicuri riguardo a qualsiasi aspetto della protezione dei dati.

CONSERVAZIONE DEI DATI

Queste regole descrivono come e dove i dati devono essere archiviati in modo sicuro. Eventuali quesiti sulla memorizzazione sicura dei dati possono essere indirizzate all'Amministratore di sistema o al Titolare.

I dati personali archiviati su carta devono essere conservati in un luogo sicuro dove le persone non autorizzate non possano accedere.

Queste linee guida si applicano anche ai dati personali che vengono solitamente archiviati elettronicamente, ma per qualche motivo sono stati stampati:

- se non richiesto, la carta o i file devono essere conservati in un cassetto o in uno schedario chiuso a chiave.
- i dipendenti devono assicurarsi che la carta e le stampe non vengano lasciate dove persone non autorizzate potrebbero vederle, per esempio in una stampante.
- le stampe dei dati devono essere triturate e smaltite in modo sicuro quando non sono più necessarie.

I dati personali archiviati elettronicamente devono essere protetti da accessi non autorizzati, cancellazioni accidentali e modifiche involontarie:

- I dati devono essere protetti da password complesse che vengono cambiate regolarmente e mai condivise tra dipendenti.
- Se i dati sono archiviati su un supporto rimovibile (come un CD, un DVD, una Pen drive o un HD esterno), questi devono essere tenuti chiusi a chiave in un luogo sicuro quando non vengono utilizzati.
- I dati devono essere memorizzati solo su unità e server designati e devono essere caricati solo su servizi di *cloud computing* approvati.
- I dati personali devono essere salvati frequentemente; questi backup dovrebbero essere testati regolarmente. I server contenenti dati personali devono essere collocati in un luogo sicuro.
- I dati personali non devono mai essere salvati direttamente (in locale) su laptop o altri dispositivi mobili come *tablet* o *smartphone*.
- Tutti i server e i computer contenenti dati personali devono essere protetti da un software di sicurezza approvato e da un *firewall*.

UTILIZZO DEI DATI

Quando lavorano con dati personali, i dipendenti devono assicurarsi che gli schermi dei loro computer siano sempre bloccati quando lasciati incustoditi.

I dati personali non devono essere condivisi in modo informale. In particolare, non devono mai essere inviati via e-mail, in quanto questa forma di comunicazione non è sicura.

I dati personali non devono mai essere trasferiti al di fuori dello Spazio economico europeo, senza seguire la corretta procedura.

I dipendenti non devono salvare copie di dati personali sui propri computer.

ACCURATEZZA DEI DATI

La legge richiede che l'Istituzione scolastica adotti misure ragionevoli per garantire che i dati siano mantenuti accurati e aggiornati.

È responsabilità di tutti i dipendenti che lavorano con dati personali adottare misure ragionevoli per garantire che siano mantenuti il più precisi e aggiornati possibile.

I dati verranno conservati solo in quanto assolutamente necessari. Il personale non deve creare *set* di dati aggiuntivi non necessari.

L'Istituzione scolastica renderà semplice per gli interessati l'aggiornamento delle informazioni che detiene su di loro (ad esempio, tramite il sito web istituzionale).

I dati devono essere aggiornati quando vengono scoperte inesattezze (ad esempio, se uno *stakeholder* non può più essere raggiunto sul numero di telefono memorizzato, dovrebbe essere rimosso dal database).

RICHIESTA D'ESERCIZIO DEI DIRITTI DELL'INTERESSATO

Tutti gli individui che sono oggetto di dati personali detenuti dall'Istituzione scolastica hanno diritto a:

- Chiedere quali informazioni l'organizzazione detiene su di loro e perché
- Chiedere la rettifica dei propri dati
- Chiedere la portabilità delle informazioni personali
- Chiederne la cancellazione
- Chiedere la limitazione od opporsi al trattamento

Le richieste d'esercizio di tali diritti da parte di soggetti devono essere inviate per e-mail, indirizzate al Titolare del trattamento all'indirizzo udic84100a@istruzione.it.

DIVULGAZIONE DEI DATI PER ALTRI MOTIVI

In determinate circostanze, il GDPR consente di divulgare i dati personali alle forze dell'ordine senza il consenso dell'interessato. In queste circostanze, l'Istituzione scolastica trasmetterà i dati richiesti. Tuttavia, il Titolare del trattamento si accerterà che la richiesta sia legittima, richiedendo assistenza al Responsabile della protezione dei dati.

FORNIRE INFORMAZIONI

L'Istituto Comprensivo I Udine si prefigge di garantire che le persone siano consapevoli del fatto che i loro dati sono trattati e che capiscano:

- come vengono utilizzati i dati
- come esercitare i loro diritti

A tal fine l'Istituzione scolastica pubblica in apposita area raggiungibile dalla home page del sito istituzionale specifiche informative sulla privacy che stabiliscono come i dati relativi alle persone sono utilizzati dall'Istituzionale scolastica.

L'Istituto Comprensivo I Udine si riserva di modificare o semplicemente aggiornare il contenuto del presente documento, anche a causa di modificazioni della normativa applicabile. Il Titolare invita quindi a visitare con regolarità la sezione Privacy del Sito per prendere cognizione della più recente versione della Politica per la protezione dei dati personali.

IL DIRIGENTE SCOLASTICO/IL TITOLARE DI TRATTAMENTO
Prof. Mauro Cecotti