POLITICA DI PROTEZIONE DEI DATI PERSONALI

L'Istituto Comprensivo raccoglie e utilizza dati personali.
Il trattamento può includere clienti, fornitori, contatti commerciali, dipendenti e altre persone con cui l'Istituto ha rapporto di tipo giuridico, economico o professionale.
La politica dell'Istituto descrive come i dati personali devono essere trattati per soddisfare gli standard di protezione delineati dal Regolamento EU 679/2016 (GDPR) e del BS 10012:2017.

SCOPO

Questa politica di protezione dei dati garantisce che l'organizzazione:

- sia conforme alla legge sulla protezione dei dati personali e secondo buone pratiche;
- protegga i diritti di personale, clienti e partner;
- sia trasparente su come raccoglie e tratta i dati personali;
- si protegga dai rischi di una violazione dei dati personali.

CAMPO DI 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)

Il Regolamento UE 679/2016 (GDPR) descrive come le organizzazioni, incluso l'Istituto Comprensivo di Sermide, 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.
Nel rispetto della normativa vigente, 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 i dati 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 un livello adeguato di protezione, ci sia una base contrattuale o siano state delineate delle BRC (Binding Corporate Rules).

Applicazione, rischi e responsabilità

Questa politica si applica all'organizzazione nel suo intero:

- Sede centrale
- Tutto il personale e i volontari
- Tutti gli appaltatori, i fornitori e tutti coloro che intrattengono rapporti professionali con I.C. di Sermide.

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

- ✓ Nomi di individui
- ✓ Indirizzi postali
- ✓ Indirizzi e-mail
- ✓ Numeri di telefono
- ✓ Qualsiasi altra informazione relativa alle persone fisiche

Rischi

Questa politica aiuta a proteggere l'organizzazione da alcuni rischi di sicurezza dei dati personali, tra cui:

- ✓ **Violazioni di riservatezza** (le informazioni personali sono state ottenute, modificate, cancellate o distribuite in modo inappropriato).
- ✓ **Impossibilità di operare una scelta** riguardo le modalità di utilizzo dei dati personali da parte dell'interessato.
- ✓ **Danno reputazionale** in caso di materializzazione di un data breach (violazione dei dati personali).

Responsabilità

Chiunque lavori per o con I.C. SERMIDE ha una certa responsabilità nel garantire che i dati personali vengano raccolti, archiviati e gestiti in modo appropriato.
Chiunque gestisca i dati personali deve garantire che siano gestiti ed elaborati in linea con questa politica e con i principi di protezione dei dati.

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

- Il **Dirigente Scolastico titolare del 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'organizzazione tiene su di loro (Vedi "**Modulo richiesta d'esercizio dei diritti dell'interessato**").
- Verificare e approvare eventuali contratti o accordi con terze parti che possano gestire i dati personali trattati dall'organizzazione.

- Il **Responsabile IT** è responsabile di:

  - Garantire che tutti 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 la scuola sta considerando di utilizzare per archiviare o elaborare dati. (Ad esempio, servizi di cloud computing).

- Il **Responsabile amministrativo Interno (DSGA)** è responsabile di:

  - Approvare qualsiasi dichiarazione sulla protezione dei dati allegata a comunicazioni quali e-mail e lettere.
  - Laddove necessario, collaborare con il Dirigente Scolastico per garantire che operazioni di carattere amministrativo rispettino i principi di protezione dei dati.

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 esigenze di lavoro**.

 I dati **non devono essere condivisi in modo informale**. Quando è richiesto l'accesso ad informazioni riservate, i dipendenti si rivolgono al Titolare del Trattamento o al Responsabile Interno.

 L'organizzazione **fornisce formazione a tutti** i dipendenti per aiutarli a comprendere le loro responsabilità nella gestione dei dati. Tale formazione è obbligatoria.

 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 aiuto** al Titolare del Trattamento o al Responsabile Interno 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. Le domande sulla memorizzazione sicura dei dati possono essere indirizzate al **Titolare**, al **Responsabile amministrativo Interno**, al **Responsabile IT**.

Quando i dati personali siano **archiviati su carta** devono essere conservati in un luogo sicuro a cui 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 venirne in contatto**, come una stampante;
- **le stampe dei dati devono essere triturate e smaltite** in modo sicuro quando non sono più necessarie.

Quando i dati personali siano **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 i dipendenti;
- ✓ se i dati **sono archiviati su un supporto rimovibile** (come un CD o un DVD), 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 **server contenenti dati personali** devono essere **collocati in un luogo sicuro**, lontano dallo spazio ufficio generale;
- ✓ i dati personali devono **essere salvati frequentemente**; questi backup dovrebbero essere testati regolarmente, in linea con le procedure di backup standard dell'organizzazione;
- ✓ 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 si lavora 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.
- È preferibile che i dati personali siano **crittografati prima di essere trasferiti elettronicamente**.
- 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**. Devono sempre accedere e aggiornare la copia centrale di tutti i dati.

Accuratezza dei dati

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

È importante che i dati personali siano accurati; l'organizzazione deve garantirne l'accuratezza.

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 posti assolutamente necessari ed adeguati**. Il personale non deve creare set di dati aggiuntivi non necessari.
- ✓ Il personale deve **cogliere ogni opportunità per garantire che i dati vengano aggiornati**.
- ✓ L'organizzazione si sforza di **rendere semplice per gli interessati l'aggiornamento delle informazioni** che detiene su di loro.
- ✓ I dati devono essere **modificati quando vengono scoperte inesattezze.**

Richiesta d'Esercizio dei diritti dell'interessato

Tutti gli individui che sono oggetto di dati personali detenuti dall'organizzazione 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 info@icsermide.gov.it. L'organizzazione fornisce un modulo di richiesta standard (Vedi **Modulo Richiesta d'esercizio dei diritti dell'interessato**), anche se gli individui non devono necessariamente utilizzarlo.

Per approfondire vedi la procedura di riferimento **P 8.1.1 Richiesta d'esercizio dei diritti dell'interessato**.

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'Organizzazione rivelerà i dati richiesti. Tuttavia, il Titolare del trattamento assicurerà che la richiesta sia legittima, richiedendo assistenza al Responsabile della protezione dei dati (**DPO**) e ai consulenti legali della società, laddove necessario.

Dare informazioni

I.C. SERMIDE mira a 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'organizzazione ha una informativa sulla privacy che stabilisce come i dati personali sono utilizzati dalla scuola.

Sermide e Felonica, 10/08/2018

IL TITOLARE DI TRATTAMENTO
Carla Sgarbi