Politica dell'IC Marconi di Altavilla Vicentina sulla privacy

Questa Istituzione raccoglie e utilizza determinati dati sulle persone. Questi possono includere personale docente e non, fornitori, e in generale soggetti esterni con cui la scuola potrebbe aver bisogno di interloquire. Questa politica descrive come questi dati personali devono essere raccolti, gestiti e archiviati per soddisfare gli standard di protezione dei dati delineati dal Regolamento EU 679/2016 (GDPR).

SCOPO

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

- Sia conforme alla legge sulla protezione dei dati personale e segue le buone pratiche
- Protegga i diritti di personale, clienti e partner
- Sia trasparente su come raccoglie e tratta i dati degli individui
- Si protegga dai rischi di una violazione dei dati personali

CAMPO DI APPLICAZIONE

Questa politica si applica ai dipendenti, collaboratori, consulenti, genitori, lavoratori temporanei, incluso tutto il personale affiliato a terze parti.

MODALITÀ OPERATIVE

Il Regolamento UE 679/2016 (GDPR)

Il Regolamento UE 679/2016 (GDPR) descrive come le organizzazioni, incluso l'IC Marconi di Altavilla Vicentina, 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 appropriate
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'istituzione nel suo intero a tutto il personale e i volontari a tutti gli appaltatori, i fornitori e le altre persone che lavorano per conto dell'istituzione. Si applica a tutti i dati che l'istituzione detiene in relazione a persone identificabili. Ciò può includere: Nomi di individui, Indirizzi postali, Indirizzi email, Numeri di telefono, altre informazioni relative alle persone.

Rischi

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

- Violazioni di riservatezza (le informazioni personali sono state 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 materializzazione di un data breach (violazione dei dati personali).

Responsabilità

Chiunque lavori per o con l'Istituto Comprensivo Marconi di Altavilla Vicentina ha una certa responsabilità nel 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 **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 o RPD) è responsabile di:

1. Mantenere il titolare di trattamento aggiornato sulle responsabilità, i rischi e le questioni relativi alla protezione dei dati.
2. Revisionare tutte le procedure di protezione dei dati e le relative politiche, in linea con un programma concordato.
3. Organizzare la formazione e la consulenza sulla protezione dei dati per le persone coperte da questa politica.
4. Gestire le domande sulla protezione dei dati da parte del personale e di chiunque altro coperto da questa politica.
5. Gestire le richieste da parte di individui per vedere i dati che l'organizzazione tiene su di loro.
6. Verificare e approvare eventuali contratti o accordi con terze parti che possano gestire i dati personali trattati dall'organizzazione

- Il **Responsabile IT (identificati nelle figure delle FS "Nuove tecnologie" e nell'Animatore digitale)** è responsabile di:

1. Garantire che tutti i sistemi, i servizi e le apparecchiature utilizzate per la memorizzazione dei dati soddisfino standard di sicurezza accettabili.
2. Eseguire controlli e scansioni regolari per garantire che l'hardware e il software di sicurezza funzionino correttamente.
3. Valutare eventuali servizi di terzi che la società sta considerando di utilizzare per archiviare o elaborare dati. (Ad esempio, servizi di cloud computing.)

- Il **Responsabile del Trattamento (identificato nella figura del DSGA)** è responsabile di:

1. Organizzare le operazioni di trattamento dei dati, effettuate dai servizi generali e amministrativo contabili, nel rispetto delle disposizioni di legge previste dal Testo Unico D.lgs 196/03, con particolare riferimento alle misure minime di sicurezza di cui all'art.31, e dal Regolamento relativo al trattamento dei dati sensibili e giudiziari
2. Vigilare sul rispetto dell'incarico attribuito e sulle istruzioni specifiche impartite a tutti gli incaricati del trattamento dei dati personali;

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 bisogno 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 chi ne fa le veci.

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'istituzione 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 a chi ne fa le veci 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. Quando i dati personali sono **archiviati su carta** devono essere conservati in un luogo sicuro dove le persone non autorizzate non possono accedervi.

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,** come in 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 dipendenti.

• Se i dati sono archiviati su un **supporto rimovibile** (come un CD o un DVD), questi dovrebbero 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 dovrebbero 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 dovrebbero mai essere inviati via e-mail, in quanto questa forma di comunicazione non è sicura.

I dati personali non dovrebbero 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'organizzazione adotti misure ragionevoli per garantire che i dati siano mantenuti accurati e aggiornati.

Più importante è il fatto che i dati personali siano accurati, maggiore è lo sforzo che l'organizzazione dovrebbe compiere per 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. Il personale non deve creare set di dati aggiuntivi non necessari.

Il personale dovrebbe cogliere ogni opportunità per garantire che i dati vengano aggiornati.

L'organizzazione renderà semplice per gli interessati l'aggiornamento delle informazioni che detiene su di loro.
I dati devono essere aggiornati 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 viic82300q@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'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

L'Istituto 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'istituzione scolastica ha una informativa sulla privacy che stabilisce come i dati relativi alle persone sono utilizzati.

Misure specifiche per la protezione dei dati		
Misura	**Office**	**Cartaceo**
Minimizzazione della quantità di dati personali L'Istituto adotta delle misure volte a gestire solo dati personali adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.	La scuola richiede sempre e solo i dati adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati. Tra l'altro per l'iscrizione è il MIUR che decide quali dati devono essere richiesti. Lo stesso per la stipula dei contratti del personale. Di conseguenza i dati richiesti vengono poi	Vengono trattati solo minimizzati

	gestiti in questo modo sia a livello informatico che cartaceo.	
Partizionamento dei dati Si adottano delle misure volte a separare le aree di archiviazione dei dati personali trattati al fine di ridurre la possibilità che i dati possano essere correlati e compromessi. Ad esempio attraverso la creazione di cartelle di rete condivise distinte per tipologia di dati personali o l'archiviazione di documentazione cartacea in faldoni o archivi separati.	I dati vengono partizionati in cartelle di rete condivise	I dati vengono suddivisi in faldoni o archivi separati.
Cancellazione sicura Si adottano misure con lo scopo di eliminare e distruggere irreversibilmente i dati personali.	E' prevista la smagnetizzazione dei supporti informatici o la distruzione di documenti cartacei, in modo che non possano essere recuperati dal supporto su cui sono archiviati.	Trita documenti

Misure generali di sicurezza fisica e logica		
Misura	**Office**	**Cartaceo**
Sicurezza dell'ambiente operativo Si adottano misure volte a gestire la configurazione di sicurezza di server e database.	I Pc hanno nome utente e password personale (non tutti posso accedere); l'accesso alle risorse di rete è controllato (non tutti possono vedere tutto)	Non applicabile
Sicurezza della rete e delle comunicazioni Si adottano misure volte a proteggere i dati personali durante il transito attraverso la rete, sia per le connessioni esterne (Internet), sia per l'interconnessione con i sistemi del MIUR. Lo strumento di protezione adottato è il firewall.	Si utilizzano connessioni protette. Gli strumenti di regolamentazione della rete (firewall) devono impedire accessi non autorizzati alla rete stessa e alle risorse.	Non applicabile

Misure generali di sicurezza fisica e logica Misure adottate da Ditta esterna		
Misura	**Office**	**Cartaceo**
Tracciatura e monitoraggio Si adottano misure per la registrazione delle attività eseguite su sistemi informatici dagli utenti e dagli amministratori di sistema su dati personali e sistemi di sicurezza, al fine di consentire il tracciamento delle operazioni svolte. Il monitoraggio delle registrazioni prodotte (c.d. "file di log"), inoltre, consente l'identificazione di potenziali tentativi interni o esterni di violazione del sistema e la rilevazione tempestiva di incidenti relativi a dati personali (ad es., eventi di diffusione, modifica o distruzione non autorizzate di dati personali), fornendo al tempo stesso gli elementi di prova nel contesto delle indagini.	E' attuata la designazione di un amministratore di sistema o un responsabile che monitora e traccia tutti i log delle attività.	Non applicabile
Gestione sicura dell'hardware, delle risorse e dei dispositivi La scuola adotta misure per gestire l'inventario e la configurazione di sicurezza dell'hardware, delle risorse di rete e dei dispositivi (server, periferiche, dispositivi di comunicazione, etc.) utilizzati per il trattamento dei dati personali.	Redazione di un inventario di chi utilizza gli strumenti in dotazione (es. pc) e che cosa utilizza.	Non applicabile
Gestione sicura delle postazioni di lavoro Vengono adottate misure per gestire la configurazione di sicurezza delle postazioni di lavoro degli utenti, fisse e portatili, (ad es., impostazioni del sistema operativo, applicazioni, software di office automation, etc.). Tali politiche impediscono agli utenti di eseguire azioni che potrebbero compromettere la sicurezza del sistema IT (ad es., la disattivazione di programmi antivirus o l'installazione e l'esecuzione di software non autorizzato, accesso a siti potenzialmente pericolosi).	Computer sicuro e verificato dall'amministratore di sistema con le precauzioni di sicurezza necessarie.	Non applicabile
Backup e Continuità operativa Esistono e vengono attuate politiche che stabiliscono le modalità di salvataggio dei dati personali, allo scopo di assicurarne la disponibilità e l'integrità nel tempo, e di ripristino dell'operatività a seguito di un evento avverso, ossia le procedure operative e	Backup In cloud o su server.	Non applicabile

le misure tecniche da seguire per ripristinare la disponibilità e l'accesso ai servizi essenziali in caso di incidente che ne pregiudichi l'operatività.		
Manutenzione delle apparecchiature Esistono e vengono attuate politiche per la manutenzione periodica delle apparecchiature di continuità elettrica, dei sistemi antincendio e di ogni altra tipologia di sistema a supporto dell'operatività dei sistemi informativi.	Controlli periodici e programmati di tutte le apparecchiature	Non applicabile

Misure organizzative e processi di governo		
Misura	**Office**	**Cartaceo**
Modello Organizzativo e di Gestione E' stato adottato un modello organizzativo e di gestione della privacy. Detto modello di gestione della privacy costituisce il fondamento per la sicurezza dei dati personali trattati dall'organizzazione, definendo i processi volti a controllare i rischi che i trattamenti dell'organizzazione pongono sui diritti e le libertà delle persone interessate e individuando ruoli e responsabilità di chi ha accesso ai dati personali, in base al principio del minimo privilegio. Un ruolo di particolare importanza è svolto dal Responsabile della Protezione dei Dati (RPD), che monitora la conformità al regolamento e collabora con il Titolare nell'adeguare le misure di protezione dei dati personali trattati.	Esempio: nomine del personale, nomina dpo, adozione di una politica sul trattamento dei dati	Esempio: nomine del personale, nomina dpo, adozione di una politica sul trattamento dei dati
Politiche e procedure per la protezione dei dati personali La politica dimostra l'impegno generale alla protezione dei dati personali e definisce i principi di base per la loro sicurezza e protezione. Il documento formalizza gli obiettivi e le regole da applicare nel campo della protezione dei dati e costituisce la base per l'attuazione delle misure tecniche e organizzative specifiche richieste dall'art. 32 del RGPD. Le specifiche misure tecniche e organizzative attuate sono descritte in procedure operative di dettaglio che indirizzano temi specifici (ad esempio controllo degli accessi, gestione dei dispositivi, gestione delle risorse, ecc.).	Adozione di una politica per la protezione dei dati personali.	Adozione di una politica per la protezione dei dati personali.

Gestione dei Responsabili del trattamento e delle terze parti Sono stati nominati con contratto o atto giuridico i rapporti con i responsabili esterni del trattamento. I rapporti con fornitori esterni di servizi che hanno accesso a o trattano dati personali per conto del Titolare devono essere formalizzati tramite un contratto o altro atto legale stabilito e siglato tra le parti, in cui è disciplinato il trattamento da parte del responsabile e specificate le misure tecniche e organizzative adottate nel rispetto dei requisiti del RGPD e a garanzia della tutela dei diritti dell'interessato.	Nomina di tutti i responsabili del trattamento	Nomina di tutti i responsabili del trattamento
Gestione degli Incidenti di sicurezza e delle Violazioni dei dati personali Nel caso si verifichino incidenti di sicurezza che comportano la "distruzione, perdita, modifica, divulgazione non autorizzata o accesso ai dati personali trasmessi, conservati o comunque trattati" (cfr. art. 4.12 del RGPD), sono attive procedure per la gestione di tali eventi e la notifica all'autorità di controllo e alle persone interessate.	Adozione di procedura per gestione data breach e predisposizione di registro e documentazione.	Adozione di procedura per gestione data breach e predisposizione di registro e documentazione.
Gestione e formazione del personale Si sono adottate misure specifiche predisposte per garantire che il personale coinvolto nel trattamento dei dati personali sia adeguatamente informato in merito agli obblighi di riservatezza. (applicabile specialmente per il personale chiave coinvolto nel trattamento dei dati personali ad alto rischio, e sensibilizzato sulle procedure di sicurezza e protezione dei dati, ad esempio uso di password e accesso a specifici sistemi di elaborazione e trasmissione dati).	Nomine persone autorizzate e formazione	Nomine persone autorizzate e formazione
Controllo degli accessi fisici Si sono adottate misure volte ad assicurare la sicurezza fisica e il controllo degli accessi agli edifici e alle zone in cui sono ospitate le risorse a supporto del trattamento (documenti cartacei e strumenti informatici). Ciò avviene attraverso un servizio di portineria con autenticazione tramite badge di riconoscimento.	Monitoraggio entrate da parte del personale	Monitoraggio entrate da parte del personale

Sicurezza dei documenti cartacei Sono state adottate e redatte politiche e processi di gestione dell'archivio per assicurare che i documenti cartacei contenenti dati personali utilizzati durante il trattamento siano prodotti, archiviati, consultati, trasmessi e distrutti nel rispetto dei diritti dell'interessato.	Non applicabile	Ambiente di archiviazione sicuro