DIREZIONE DIDATTICA 2° CIRCOLO DI FORMIGINE
Via Erri Billò, 49 – 41043 Casinalbo (Mo) - C.F. 80011570365
Tel. 059/550225
Email moee037009@istruzione.it Web www.ddformigine2.edu.it
Posta certificata: moee037009@pec.istruzione.it

Kit privacy

DIREZIONE DIDATTICA FORMIGINE 2

Sul sito dell'istituzione scolastica è rinvenibile l'INFORMATIVA completa sul trattamento dei dati personali che costituisce l'ALLEGATO 1 del presente "kit privacy"

POLICY della DD Formigine 2

La Direzione Didattica Formigine 2 quale policy della propria istituzione a tutela della privacy adotta le misure che seguono:

il personale esercita le funzioni/mansioni proprie dell'incarico solo in luoghi idonei a mantenere la riservatezza dei dati. A tal fine non è consentito raccogliere, archiviare o inviare dati personali, in luoghi o destinazioni che per la loro conformazione, non consentano un adeguato livello di privacy. E' severamente vietato divulgare i dati trattati e di cui si è venuti a conoscenza in funzione del proprio ruolo, ad esempio, a mezzo telefono, chat o social media. Quanto al telefono, qualora sia necessario comunicare alcuni dati ad altri soggetti autorizzati, bisognerà aver cura di non essere ascoltati da terzi, mantenendo sempre un tono di voce moderato ed assicurarsi che le porte dell'ufficio siano chiuse o che la comunicazione necessaria, in virtù del proprio compito, sia resa tenendo conto dell'adeguato grado di riservatezza richiesto. E' obbligatorio utilizzare strumenti dotati di adeguati sistemi di protezione da rischio informatico. E' obbligatorio utilizzare sistemi operativi aggiornati o evidenziarne l'obsolescenza affinché siano sostituiti o aggiornati. E' fatto divieto di utilizzare, per finalità istituzionali, indirizzi e-mail con domini non istituzionali. Sui device scolastici è vietato installare qualsiasi programma non strettamente essenziale alla raccolta ed archiviazione dei dati. In ogni caso è severamente vietato condividere i nomi ed i dati con chiunque, compresi possibili partner, collaboratori, fornitori o esterni, in mancanza di una autorizzazione espressa da parte dell'interessato. Questa previsione non si applica alle comunicazioni tra soggetti autorizzati al trattamento dei dati in virtù dell'esercizio del proprio ufficio. E' fatto divieto di archiviare i dati su cloud non istituzionali.

Il personale amministrativo deve allestire la postazione di lavoro in modo da garantire la riservatezza dei dati ed effettuare il log-out dai servizi/portali utilizzati dopo che è stata conclusa la sessione lavorativa. Al fornitore dei servizi informatici è richiesto di Implementare sistemi di backup, prediligendo servizi cloud o dispositivi di archiviazione cifrati (es. pen drive e hard disk esterni).

Utilizzo dei propri device (BYOD)

Con "device" si intende qualsiasi strumento elettronico capace di raccogliere, archiviare e/o trasmettere dati. Rientrano in questa categoria, a mero titolo esemplificativo, computer, tablet, smartphone, smartwatch, agende elettroniche. Al personale è chiesto di servirsi prioritariamente dei device di proprietà della scuola i quali dovranno peraltro essere utilizzati esclusivamente per i fini istituzionali; qualora un dipendente vorrà utilizzare un proprio device per lo svolgimento di attività istituzionali gli è richiesto di attenersi alle seguenti indicazioni:

Assicurarsi di accedere al sistema operativo con un account riservato all'attività istituzionale e dotato di password sicura. Se si tratta di computer usato da altri, compresi altri membri della famiglia, costoro dovranno connettersi utilizzando un'utenza diversa, anche sul medesimo device. E' vietato utilizzare l'accesso a connessioni Wi-Fi che non richiedano la procedura di verifica e riconoscimento dell'utente.

Sito Internet

La gestione del sito è affidata a NUVOLA MADISOFT. Il sito deve essere allocato su server in unione europea. Il sito non deve contenere alcun cookie analitico, marketing o di profilazione. Sono concessi i soli cookie tecnici di sessione. Il sito non può contenere form privi del rimando all'informativa e, ove necessario, della richiesta di adeguato consenso. Sul sito non devono essere promossi eventi diversi da quelli riconducibili alle finalità istituzionali. Sul sito non devono essere pubblicate foto senza prima richiedere gli opportuni consensi, né sulle Classroom. Sarà cura ed obbligo dei docenti accertarsi che siano stati firmati i documenti (da entrambi i genitori/tutori) e che sia reso il consenso espresso alla pubblicazione di foto/video che in ogni caso rientrino nelle attività istituzionali della scuola e comprese nel Ptof. Per la creazione di eventuali newsletter è necessario che le stesse siano pensate in modo da garantire la presenza di idonea informativa e la raccolta dei necessari consensi, con particolare attenzione alla possibilità di richiedere in qualsiasi momento la cancellazione dall'elenco degli iscritti alla newsletter stessa.

Data Breach

Il DATA BREACH è una violazione della sicurezza che comporta accidentalmente o illegalmente - la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali, trasmessi, archiviati o altrimenti elaborati. In caso di violazione l'Istituzione deve denunciare il sinistro al Garante privacy. Per questo motivo, in caso di data breach il personale che vi è occorso o che ne abbia notizia è tenuto a comunicare l'evento tempestivamente al dirigente scolastico affinché possa immediatamente interfacciarsi con Corporate per i provvedimenti del caso, entro e non oltre 10 ore dalla conoscenza del fatto.

Quali eventi costituiscono un Data Breach:

- furto di credenziali di autenticazione a seguito di un attacco di phishing;
- perdita di una chiavetta USB o di un telefono cellulare o laptop con conseguente perdita di documenti contenenti dati personali;
- cancellazione accidentale o pubblicazione indesiderata di un database su Internet;
- accesso a informazioni riservate da parte di utenti non autorizzati.

PROCEDURA PER GESTIRE VIOLAZIONE DEI DATI

PRIMA FASE- **Valutazione e contenimento: primi 10 minuti** dalla conoscenza del fatto. In caso di incidente di sicurezza (accertato o sospetto), SI PROCEDE COME SEGUE:

1. Chiamare/comunicare immediatamente il sinistro al Dirigente Scolastico, il quale contatterà il DPO.
2. Interrompere la perdita di dati aggiuntivi: portare offline le macchine interessate, ma non disattivarle.
3. Disattivare quindi il Wi-Fi o scollegare il cavo Ethernet dal laptop.
4. Registrare il momento della scoperta: inviare una mail a belmonte.cristina@ddformigine2.edu.it con OGGETTO: URGENTE DATA BREACH con le seguenti informazioni: chi ha scoperto la violazione, chi l'ha segnalata, a chi è stata segnalata, chi altro ne è a conoscenza e che tipo di violazione si è verificata

SECONDA FASE - Report: i successivi 20 minuti dalla conoscenza del fatto. Il soggetto (o i soggetti) che ha scoperto la violazione dei dati personali deve poi annotare:

- il dispositivo interessato, nonché la causa e l'entità;

- le categorie e il numero approssimativo di persone interessate;
- le categorie e il volume approssimativo di dati personali interessati;
- una descrizione delle possibili conseguenze della violazione dei dati personali.
    - Inviare e-mail con le informazioni di cui sopra a belmonte.cristina@ddformigine2.edu.it

Attività degli Uffici

Agli Uffici che effettuano attività di trattamento di dati personali nell'ambito della propria operatività è richiesto con periodicità di verificare che tutto il personale di cui trattano i dati abbia ricevuto la modulistica prescritta (INFORMATIVA BREVE e CONSENSO TRATTAMENTO DATI – ALLEGATI 2 E 3, 4 e 5- modulistica rinvenibile a sul sito oltre che a disposizione in ogni ufficio in modalità cartacea)

Ufficio ALUNNI

- verificare, ove necessario in relazione alla finalità perseguita, l'acquisizione dei **consensi al trattamento e rendere le informative al momento dell'iscrizione;**
- tenere aggiornato database fascicolo alunni (consenso al trattamento dei dati)
- conservazione sottochiave dei consensi firmati laddove cartacei.

Ufficio PERSONALE DOCENTE

- verificare, ove necessario in relazione alla finalità perseguita, l'acquisizione dei **consensi al trattamento da acquisire all'atto della sottoscrizione dei contratti**
- acquisizione del consenso al trattamento dei dati annualmente da parte del personale in servizio (inizio anno scolastico)
- **tenere aggiornato database della modulistica acquisita conservata digitalmente (con password di accesso), in formato cartaceo in armadio chiuso a chiave**

Ufficio PERSONALE ATA

- verificare, ove necessario in relazione alla finalità perseguita, l'acquisizione dei **consensi al trattamento da acquisire all'atto della sottoscrizione dei contratti**
- acquisizione del consenso al trattamento dei dati annualmente (inizio anno scolastico) da parte del personale in servizio
- **tenere aggiornato database della modulistica acquisita conservata digitalmente (con password di accesso), in formato cartaceo in armadio chiuso a chiave**

Ufficio AFFARI GENERALI

- verificare, ove necessario in relazione alla finalità perseguita, l'acquisizione dei **consensi al trattamento da acquisire all'atto della sottoscrizione dei protocolli firmati con tirocinanti e volontari**
- **tenere aggiornato database della modulistica acquisita conservata digitalmente (con password di accesso), in formato cartaceo in armadio chiuso a chiave**

Ufficio ACQUISTI

- verificare che al contratto sottoscritto sia allegata l'Informativa per il trattamento dei dati;
- in caso di nomina di responsabile esterno di un servizio (esperto esterno, psicologo, educatore) verificare che sottoscriva il modulo per il trattamento dei dati personali e l'assunzione di responsabilità in merito ai dati che tratta in funzione del proprio incarico.
- **L'assistente amministrativo incaricato all'Ufficio acquisti dovrà curare:**
- ELENCO FORNITORI
- NOMINA ALL'INCARICO
- INFORMATIVA PRIVACY e CONSENSO
- Data base dell'ANAGRAFICA FORNITORI
- NOMINA INCARICO RESPONSABILE ESTERNO e prescritta modulistica per assunzione di responsabilità del trattamento dei dati.

PERSONALE DOCENTE

- verificare, ove necessario in relazione alla finalità perseguita, l'acquisizione dei **consensi al trattamento dei dati personali da parte di entrambi i genitori/tutori degli alunni della propria classe (Informativa breve alunni, ALLEGATO)**
- tenere aggiornato database della modulistica acquisita conservata digitalmente (con password di accesso), se in formato cartaceo custodita in armadio o cassetto chiuso a chiave;
- custodire il protocollo di somministrazione farmaci garantendo la massima tutela poiché tratta dati sensibilissimi legati allo stato di salute, proteggendo l'identità dell'alunno da accessi non autorizzati;
- elaborare eventuale lista di eventuali dinieghi a uno o più trattamenti
- tenere a mente che in caso di consenso disgiunto prevale la misura più restrittiva.

Raccolta di dati tramite QUESTIONARI PER ATTIVITÀ DI RICERCA

La raccolta di informazioni personali, spesso anche sensibili, per attività di ricerca effettuate da soggetti legittimati attraverso questionari **è consentita soltanto se i ragazzi, o i genitori nel caso di minori, sono stati preventivamente informati sulle modalità di trattamento e conservazione dei dati raccolti e sulle misure di sicurezza adottate**. Studenti e genitori devono comunque essere lasciati liberi di non aderire all'iniziativa. La raccolta di tali informazioni è consentita unicamente mediante acquisizione del consenso espresso sottoscritto da entrambi i genitori.

Strategia adottata a garantire la **protezione dei dati:**

- archiviazione digitale protetta da accesso riservato
- custodia della documentazione cartacea in faldoni riposti sotto chiave

CRITERI PER IL TRATTAMENTO DEI DATI:

- liceità (trattamento di dati indispensabili per le finalità dell'ufficio)
- correttezza e trasparenza (l'interessato deve sapere che sto trattando dati che gli appartengono)
- minimizzazione (solo dati indispensabili)

- integrità (i dati sono solo collezionati)
- riservatezza (i dati sono custoditi e conosciuti solo in virtù dell'ufficio e dell'obbligo di doverli trattare)
- limitazione della conservazione (durata limitata della conservazione del dato)

I dati personali sono raccolti e conservati solo **se le finalità dei trattamenti non sono ragionevolmente conseguibili con altri mezzi**, sono processati e conservati in modo **proporzionato** agli scopi per i quali vengono raccolti. In riferimento all'art. 5, paragrafo 1 **GDPR il periodo di conservazione dei dati personali è limitato al minimo necessario** e proporzionato agli scopi per i quali sono raccolti i dati.

DPO

Il DPO designato per la DIREZIONE DIDATTICA FORMIGINE 2 è Corporate Studio. La modulistica privacy è rinvenibile sul sito dell'istituzione scolastica.

IL DIRIGENTE SCOLASTICO

Dott.ssa Cristina Belmonte

Documento informatico sottoscritto con

firma digitale ai sensi del D. Lgs. n. 82/2005 e ss.mm.ii