



POLICY privacy dell' IC SOLIERA

in materia di protezione dei dati personali (GDPR) e nel rispetto del Regolamento privacy

IL DIRIGENTE SCOLASTICO

VISTI

- il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 (GDPR);
- il Decreto Legislativo 30 giugno 2003, n. 196, recante “Codice in materia di protezione dei dati personali”, come modificato dal D.Lgs. 10 agosto 2018, n. 101;
- gli articoli 29 e 32 del Regolamento (UE) 2016/679, relativi agli autorizzati al trattamento e alle misure di sicurezza;
- il Decreto Legislativo 7 marzo 2005, n. 82 (Codice dell'Amministrazione Digitale);
- il Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445;
- il Decreto Legislativo 14 marzo 2013, n. 33, come modificato dal D.Lgs. 97/2016, in coordinamento con la normativa sulla protezione dei dati personali;
- le Linee guida e i provvedimenti del Garante per la protezione dei dati personali in materia di trattamento dei dati in ambito scolastico;
- il Contratto Collettivo Nazionale di Lavoro del comparto Istruzione e Ricerca vigente;
- il PTOF dell'Istituto Comprensivo;
- il Regolamento di Istituto;
- il Regolamento interno per la protezione dei dati personali;
- **gli indirizzi, le raccomandazioni e le linee guida emanate dalla Regione Emilia-Romagna in materia di protezione dei dati personali**, applicabili, per quanto compatibili, ai servizi e alle attività educative e scolastiche, in coerenza con il Regolamento (UE) 2016/679 (GDPR) e con la normativa nazionale vigente;

CONSIDERATA

- la necessità di garantire la tutela dei dati personali di alunni, famiglie, personale e soggetti terzi;
- la rilevanza del corretto trattamento dei dati personali, in particolare di quelli relativi a minori;

RICHIAMATO

- il principio di responsabilizzazione (“accountability”) dei soggetti autorizzati al trattamento;

EMANA LA SEGUENTE DIRETTIVA

Art. 1 – Ambito di applicazione

La presente Direttiva si applica a tutto il personale dell'Istituto Comprensivo, docente e ATA, nonché a ogni altro soggetto che, a qualsiasi titolo, tratti dati personali per conto dell'Istituzione scolastica.

Art. 2 – Obblighi del personale

Tutto il personale è tenuto a:

Firmato digitalmente da CRISTINA BELMONTE

- trattare i dati personali esclusivamente per finalità istituzionali e nel rispetto delle istruzioni ricevute;
- adottare comportamenti improntati a riservatezza, correttezza e sicurezza;
- custodire con diligenza documenti, credenziali e strumenti informatici;
- evitare comunicazioni o diffusioni non autorizzate di dati personali, in particolare se riferiti a minori o a categorie particolari di dati;
- segnalare tempestivamente eventuali violazioni o sospetti di violazione dei dati personali (data breach).
- Ad informarsi al riguardo delle misure e dei comportamenti da adottare al riguardo della presente direttiva che ha carattere permanente ed è pubblicata all'Albo della scuola e nella bacheca delle circolari del personale docente ed ATA.

Art 3 Misure da adottare

L'IC Soliera adotta quale propria policy privacy 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. In uso di strumenti informatici propri è obbligatorio utilizzare strumentazioni dotate di adeguati sistemi di protezione da rischio informatico (antivirus aggiornato, firewall). 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).

L'IC di Soliera adotta il Registro delle attività di trattamento, in ottemperanza all'Art. 30 GDPR.

Art .4 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. Il personale, per lo svolgimento delle attività istituzionali e per le attività in classe dovrà servirsi prioritariamente dei device di proprietà della scuola (utilizzati peraltro esclusivamente per i fini istituzionali). Nell'utilizzo di device proprio, ciascun lavoratore dovrà accertarsi di:

accedere al sistema operativo con un account riservato all'attività istituzionale e dotato di password sicura;

assicurarsi che i propri dispositivi siano protetti (ad es. utilizzando cifratura, protezione con Pin, VPN);

utilizzo esclusivo binario device-utenza (se il computer è usato da altri, compresi altri membri della famiglia, costoro dovranno connettersi utilizzando un'utenza diversa sul medesimo device).

Art. 5 DIVIETI

E' vietato utilizzare l'accesso a connessioni Wi-Fi che non richiedano la procedura di verifica e riconoscimento dell'utente.

È vietato fare ricorso a cloud non istituzionali: Si afferma che è vietato archiviare dati su cloud non istituzionali e sono ammessi solamente quelli con sede in UE e conformi al GDPR.

Art. 6 Sito Internet

La gestione del sito è affidata esternamente 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, non è consentito nemmeno sulle Classroom se non per attività istituzionali e per questo autorizzate dagli interessati. 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 o blog 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.

Art. 7 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 Spaggiari "Progetto Privacy" per i provvedimenti del caso, entro e non oltre 48 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 20 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 cristina.belmonte@icsoliera.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: cristina.belmonte@icsoliera.edu.it

Art. 8 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- modulistica rinvenibile a sul sito oltre che a disposizione in ogni ufficio in modalità cartacea)

Ufficio ALUNNI

Firmato digitalmente da CRISTINA BELMONTE

- 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.
- La documentazione riguardante dati particolari (es. quelli sulla salute degli alunni, come il protocollo di somministrazione farmaci) è conservata ed archiviata utilizzando misure quali la cifratura.

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.**
- La documentazione riguardante dati particolari (es. quelli sulla salute degli alunni, come il protocollo di somministrazione farmaci) è conservata ed archiviata utilizzando misure quali la cifratura.

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.

Art. 9 diligenza del 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

Firmato digitalmente da CRISTINA BELMONTE

- tenere a mente che in caso di consenso disgiunto prevale la misura più restrittiva.
- La documentazione riguardante dati particolari (es. quelli sulla salute degli alunni, come il protocollo di somministrazione farmaci) è conservata ed archiviata e conservata in luogo sicuro anche utilizzando misure quali la cifratura.

Art. 9 , lett.a 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. Qualunque richiesta di compilazione di questionari deve essere autorizzata dal Dirigente scolastico.

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 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)

Art. 10 SANZIONI PER INOSSERVANZA

L'inosservanza delle disposizioni contenute nel Regolamento interno sulla protezione dei dati personali, nonché delle norme previste dal Regolamento (UE) 2016/679 (GDPR) e dal D.Lgs. 196/2003 e s.m.i., comporta l'applicazione di sanzioni disciplinari, ferme restando eventuali responsabilità civili, penali e amministrative. Le sanzioni sono comminate in relazione alla **gravità della violazione**, alla **recidiva**, al **grado di responsabilità** e all'eventuale **danno arrecato agli interessati o all'Istituzione scolastica**. L'applicazione delle sanzioni disciplinari avviene nel rispetto delle procedure previste dal **CCNL di riferimento**, dalla normativa vigente e dal principio di proporzionalità. Restano salve le eventuali segnalazioni all'Autorità Garante per la protezione dei dati personali e l'adozione di ulteriori provvedimenti previsti dalla legge.

Disposizioni finali

Per quanto non espressamente previsto dalla presente Direttiva, si rinvia alle disposizioni del Regolamento (UE) 2016/679 (GDPR), del D.Lgs. 196/2003 e s.m.i., ai provvedimenti e alle linee guida del Garante per la protezione dei dati personali, nonché alla restante normativa vigente in materia. Le disposizioni della presente Direttiva si applicano in modo coordinato e compatibile con il Regolamento di Istituto, il Regolamento interno sulla protezione dei dati personali, il PTOF e gli altri atti interni dell'Istituzione scolastica, che restano pienamente efficaci. Essa potrà essere aggiornata o integrata con successivi atti del Dirigente scolastico, anche in relazione a modifiche normative, a nuovi indirizzi delle Autorità competenti o a esigenze organizzative dell'Istituzione scolastica. E' resa conoscibile a tutto il personale mediante pubblicazione agli atti dell'Istituto, pertanto la conoscenza delle disposizioni in essa contenute è presunta a seguito della pubblicazione. La Direttiva entra in vigore dalla data di pubblicazione ed è immediatamente vincolante per tutto il personale dell'Istituto Comprensivo.

Il DPO designato per l' IC Soliera è Spaggiari Giampaolo "Progetto Privacy srl".

f.to IL DIRIGENTE SCOLASTICO

Dott.ssa Cristina Belmonte

Firmato digitalmente da CRISTINA BELMONTE