I. C. GEMITO ANACAPRI
Via Pagliaro, 7/A – 80071 Anacapri (NA)
Cod. Simpi: NAIC83600Q – Cod. Fisc. 90044580638 Cod. Unico Ufficio UFFIGQ
Tel. 081 8371247
e-mail NAIC83600Q@istruzione.it/NAIC83600Q@pec.istruzione.it
Web Site: www. istitutocomprensivogemito.edu.it

Regolamento interno
Data – Protection Policy

SOMMARIO

1. SCOPO

Il Titolare del trattamento è Istituto Comprensivo Statale V. Gemito di Anacapri, in persona del Dirigente scolastico p.t. Prof.ssa Rossella Ingenito, con sede in Via Pagliaro 7/A - 80071 Anacapri (Na) (Tel.: 0818371247; pec: naic83600q@pec.istruzione.it), cui lei potrà in ogni momento rivolgersi per esercitare i suoi diritti o semplicemente richiedere in-formazioni relative al trattamento dei suoi dati utilizzando questi recapiti diretti: Email: naic83600q@istruzione.it; PEC: naic83600q@pec.istruzione.it
Inoltre, il Titolare ha nominato, come previsto dal DPGR 679/2016, il Responsabile della protezione dei dati (RPD) individuandolo nella persona: avv. Elio Errichiello al quale rivolgersi direttamente utilizzando i seguenti recapiti diretti: mail: elio.errichiello@gmail.com
Al fine di garantire all'interno della Scuola puntuale applicazione del "Codice in materia di protezione dei dati personali" (D. Lgs. 30 giugno 2003 n. 196) e successive modifiche e/o integrazioni anche ai sensi del Regolamento UE (GDPR) 2016/679 e di ridurre al minimo i rischi per la protezione dei dati si emanano le seguenti linee guida con lo scopo di garantire che il trattamento dei dati personali avvenga nel rispetto dei diritti e delle libertà fondamentali delle persone, con particolare riferimento a tutti gli interessati che hanno rapporti con la Scuola.
A tale scopo la presente policy definisce i principi che disciplinano la protezione dei dati nella Scuola.

2. DEFINIZIONI

Al fine della presente policy, si intende per:
1) «**dato personale**»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

2) «**trattamento**»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

3) «**limitazione di trattamento**»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

7) «**titolare del trattamento**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

8) «**responsabile del trattamento**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

9) «**destinatario**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nel- l'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

10) «**terzo**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

11)«**consenso dell'interessato**»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

12) «**violazione dei dati personali**»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

21) «**Garante**»: l'autorità pubblica indipendente istituita a presidio del diritto alla protezione dei dati personali;

Per tutte le altre definizioni si fa espresso richiamo all'art.4 del GDPR.

3. AMBITO DI APPLICAZIONE

La presente policy si applica a tutti i trattamenti di dati personali effettuati da singole persone, in particolare da dipendenti, clienti, fornitori o altri partner contrattuali.

4. VALUTAZIONE DEL RISCHIO

Le violazioni della protezione dei dati possono comportare gravi conseguenze giuridiche ed economiche per le imprese, i loro dipendenti o le persone interessate. Possono anche danneggiare l'immagine dell'amministrazione, far perdere fiducia ai clienti e ad altri partner contrattuali e avere potenziali conseguenze sul piano del diritto del lavoro per i dipendenti.
L'attuazione di quanto previsto dagli artt. 33-34 del Regolamento UE 2016/679 in merito alla procedura operativa di Analisi e Gestione della Notifica del Data Breach riduce al minimo i rischi per la protezione dei dati.
La Scuola, in caso di Data Breach, si impegna a seguire le procedure indicate dagli artt. 33-34 del Regolamento UE 2016/679.

5. PRINCIPI DELLA PROTEZIONE DEI DATI

I dati personali devono essere trattati in modo lecito e in modo da salvaguardare il diritto alla protezione dei dati personali dell'interessato. In tale contesto, la Scuola si attiene principi di protezione dei dati previsti dal GDPR ed in particolare:
- principio di finalità: i dati personali possono essere trattati solo per le finalità definite prima della loro raccolta. Successive modifiche allo scopo che non hanno una stretta connessione oggettiva con lo scopo originale sono possibili solo in misura limitata. Esse possono essere effettuate solo con il consenso della persona interessata, in base ad accordi previsti da un contratto collettivo o dalla legislazione nazionale o dalla legislazione dell'UE;
- principio di proporzionalità: il trattamento dei dati è proporzionato solo se è adeguato, necessario e ragionevole per conseguire una finalità legittima e se non vi si oppone la tutela di superiori diritti e libertà dell'interessato;
- principio di trasparenza: gli interessati devono essere informati dal titolare del trattamento, in modo chiaro e adeguato, dei loro dati personali oggetto di trattamento;

- principio di necessità: i dati personali devono essere trattati nella misura necessaria al raggiungimento dello scopo previsto dal trattamento stesso. È preferibile utilizzare I dati anonimi, qualora lo scopo possa essere ugualmente raggiunto e se lo sforzo richiesto sia ragionevole; i dati personali non possono essere raccolti in anticipo e conservati per potenziali finalità future, a meno che ciò non sia previsto dalla legislazione nazionale; i dati che non sono più necessari devono essere cancellati; il trattamento deve essere bloccato durante il tempo necessario per la loro cancellazione (cfr. par. 7 della presente policy);
-qualità dei dati: i dati personali devono essere raccolti e trattati in modo da essere oggettivamente corretti. Devono essere adottate misure adeguate per garantire che i dati errati o incompleti siano immediatamente corretti, integrati o cancellati.
Inoltre, soggetti autorizzati hanno accesso ai dati personali limitatamente alla natura e alla portata dei loro compiti. Qualsiasi trattamento effettuato da persone non incaricate di farlo nell'ambito dei loro compiti e senza il possesso di un'autorizzazione appropriata non è autorizzato. In particolare, i dati personali non devono essere trasferiti o messi a disposizione di persone non autorizzate.

6. TRASFERIMENTO DEI DATI

I dati personali devono essere trasferiti a terzi con il consenso della persona interessata, dopo averla chiaramente informata in ordine alle finalità, alla natura del trattamento all'identità dei destinatari e alla base legale che giustifica tale trasferimento. Qualora i dati siano trasferiti al di fuori dell'UE è opportuno verificare che il Paese terzo offra un'adeguata protezione in materia di protezione dei dati personali e, se del caso, ricorrere ad apposite clausole standardizzate o norme vincolanti di impresa, come previsto al Capo V del GDPR in materia di trasferimenti transfrontalieri.

7. DIRITTI DEGLI INTERESSATI

In caso di trattamento di dati personali, gli interessati devono esserne a conoscenza in tempo utile, così come deve essere agevolmente e rapidamente garantito l'esercizio dei loro diritti di cui agli artt. da 15 a 22 del GDPR:

Diritto di accesso

L'interessato ha il diritto di ottenere dal Titolare del trattamento la conferma dell'esistenza o meno di dati personali che lo riguardano anche se non ancora registrati e la messa a disposizione dei medesimi in forma intelligibile; ha inoltre il diritto di conoscere l'origine dei dati, la logica e le finalità su cui si basa il loro trattamento.

Diritto di rettifica

L'interessato ha il diritto di ottenere l'aggiornamento, la rettifica o, qualora vi abbia interesse, l'integrazione dei dati medesimi; ha altresì il diritto di opporsi in tutto o in parte, per motivi legittimi, al trattamento dei propri dati personali ancorché pertinenti allo scopo della raccolta, il diritto di limitazione del trattamento e il diritto di opporsi a un processo decisionale automatizzato.

Diritto alla portabilità dei dati

L'interessato ha il diritto alla portabilità dei propri dati personali a partire dal 25 maggio 2018.

Diritto alla cancellazione

La Scuola conserva i dati personali solo per il tempo necessario a fornire il servizio o per obblighi di legge; diversamente l'interessato può ottenerne la cancellazione (cfr. par. 7 della presente policy).

Diritto di opporsi al trattamento

Tale diritto può essere effettuato sulla base di decisioni completamente automatizzate, ossia prese senza alcun intervento umano, che producano effetti giuridici che lo riguardano. All'interessato dovrà essere sempre garantito il diritto di ottenere l'intervento umano nella valutazione e di poter contestare la decisione.
Per garantire tali diritti dal punto di vista tecnico occorre che gli addetti all'amministrazione scolastica siano pronti a recepire le richieste inoltrate dagli interessati, inviate a mezzo mail o con altro mezzo, e inoltrarle

ai diretti responsabili, ovvero in mancanza al Dirigente scolastico nella qualità di Titolare, per la risoluzione di qualsivoglia domanda in termini ragionevoli.

8. RUOLI E RESPONSABILITÀ

Gli organi direttivi della Scuola e i singoli incaricati sono responsabili del rispetto delle disposizioni di legge e aziendali in materia di tutela dei consumatori.
Anche i dipendenti hanno una responsabilità individuale in tal senso nell'ambito dell'adempimento dei loro compiti.

9. SICUREZZA DEI DATI

I dati personali oggetto di trattamento devono essere custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati ed alle specifiche caratteristiche del trattamento, in modo tale da ridurre al minimo, mediante l'adozione di idonee misure di sicurezza, i rischi di distribuzione o di perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito non conforme alle finalità di raccolta.
Ai sensi e per gli effetti di cui sopra, la Scuola detiene il **Regolamento per il corretto utilizzo del sistema informatico**, aggiornato annualmente.
Nel campo della sicurezza dei dati il D.S.G.A. avrà il compito di generare, sostituire ed invalidare, in relazione agli strumenti ed alle applicazioni informatiche utilizzate, la parola chiave ed i codici di accesso personali da assegnare agli incaricati del trattamento dei dati, nel rispetto delle massime misure di sicurezza.
La Scuola dovrà adottare adeguati **programmi antivirus, firewall ed altri strumenti software o hardware atti a garantire la massima misura di sicurezza** nel rispetto di quanto dettato dal D.Lgs.196/2003, nonché dal Regolamento UE 2016/679 al Capo IV ed utilizzando le conoscenze acquisite in base al progresso tecnico di software ed hardware.

Lo stesso D.S.G.A. avrà il compito di controllare periodicamente l'efficienza dei sistemi tecnici adottati e di redigere apposita relazione, da consegnare al Dirigente Scolastico, in qualità di Titolare, riportante i riscontri e le verifiche effettuate, i parametri adottati e gli accorgimenti proposti per migliorare la sicurezza. Inoltre dovrà:

• prendere tutti i provvedimenti necessari ad evitare la perdita o la distruzione dei dati e provvedere al ricovero periodico degli stessi con copie di back – up;

• assicurarsi della qualità delle copie di back-up dei dati e della loro conservazione in luogo adatto e sicuro;

• fare in modo che sia prevista la disattivazione dei Codici identificativi personali (USER- ID), in caso di perdita della qualità che consentiva all'utente o incaricato l'accesso all'elaboratore, oppure nel caso di mancato utilizzo dei Codici identificativi personali, per oltre sei mesi:

• garantire il rispetto di tutte le misure di sicurezza per i trattamenti elettronici specificate all'art.34 del Codice ed al relativo allegato B), nonché dal GDPR;

• indicare al personale competente o provvedere direttamente alla distruzione o allo smaltimento dei supporti informatici di memorizzazione logica o alla cancellazione dei dati per il loro reimpiego.

10. UTILIZZO DEGLI STRUMENTI DI LAVORO AZIENDALI

Per quanto riguarda gli strumenti elettronici ed informatici, occorre ricordare che se forniti dalla Scuola (es. la casella di posta elettronica) sono dotazioni aziendali e quindi controllabili dal datore ed inutilizzabili a fini personali. Di contro, la mail privata del dipendente, in quanto è dato personale ed è uno strumento identificativo, non è mai controllabile dalla Scuola anche se utilizzata dal luogo di lavoro.

La navigazione in Internet tramite gli strumenti aziendali può essere limitata o vietata purché non sussista un trattamento illecito dei dati dei lavoratori. Quindi, possono essere applicati appositi filtri per impedire gli accessi a determinati siti, ma i sistemi devono essere configurati in modo da cancellare periodicamente i dati personali (accessi ai siti). Un monitoraggio sistematico della navigazione su Internet dei lavoratori deve ritenersi illecito.
Le risorse umane, oltre ad avere il diritto alla protezione dei propri dati personali, hanno un dovere di trattare in modo lecito e sicuro i dati personali altrui nel contesto delle loro attività lavorative.
A tal proposito è necessario investire sulla formazione dei dipendenti e sensibilizzarli sul tema della privacy e della sicurezza dei dati nei luoghi di lavoro.
È imposto poi ad ogni dipendente di seguire le istruzioni delineato a tal proposito nel Documento "*Regolamento per l'utilizzo dei sistemi informatici*", allegato alla presente policy.
Per ciò che concerne l'utilizzo di **documenti cartacei**, i dipendenti sono tenuti ad effettuare copie e conservare gli stessi con la massima diligenza in modo da garantire la sicurezza e la riservatezza delle informazioni negli stessi contenute. I documenti contenti dati comuni devono essere chiusi in **armadi sotto chiave** con accesso al personale autorizzato. I documenti contenti dati sensibili e sanitari devono essere chiusi in **cassaforte** con accesso al personale autorizzato.

11. NORME DI RINVIO

Fermo restando quanto previsto nella presente policy, per il trattamento dei dati personali, trovano comunque applicazione tutte le disposizioni contenute nel D.Lgs. 30 giugno 2003, n. 196 e nel Regolamento UE 2016/679, nonché provvedimenti e linee guida del Garante per la protezione dei dati personali.

Il Dirigente Scolastico
(Rossella Ingenito)
Firma autografa sostituita a mezzo stampa
(art. 3, comma 2 del decreto legislativo n. 39/1993)