IC Ovest 2 Brescia

Via Interna 22, 25127 Brescia Tel: 030 301366
Codice IPA: istsc_bsic886005
PEO: BSIC886005@istruzione.it PEC BSIC886005@PEC.istruzione.it

Prot. e data vedi file di segnatura

Agli Assistenti Amministrativi
DSGA
SEDE
Albo
Sito WEB

Oggetto: protezione dei dati personali ex Regolamento UE 2016/679 - designazione incaricati Struttura operativa: **Segreteria**

IL DIRIGENTE

1. VISTO il Regolamento UE 2016/679 con riguardo agli artt. 24, 29 e 32;
2. VISTO l'Art. 2 quaterdecies del Codice Privacy Attribuzioni di funzioni e compiti a soggetti designati;
3. CONSIDERATO che questo Istituto è titolare del trattamento dei dati personali di alunni, genitori, personale dipendente, fornitori, e qualunque altro soggetto che abbia rapporti con l'Istituto medesimo e che a questo conferisca, volontariamente o per obbligo, propri dati personali;
4. CONSIDERATO che la titolarità del trattamento dei dati personali è esercitata dallo scrivente Dirigente dell'Istituto, in qualità di legale rappresentante dello stesso;
5. CONSIDERATO che le SS.LL. prestano servizio presso questo Istituto come addetti alla Struttura operativa: Area Segreteria, ferma restando ogni responsabilità civile e penale;
6. CONSIDERATO che vanno individuati gli Autorizzati al trattamento. La nomina a Autorizzato non implica l'attribuzione di funzioni ulteriori rispetto a quelle già assegnate bensì soltanto ricevere un'autorizzazione a trattare dati personali e istruzioni sulle modalità cui attenersi nel trattamento.
7. CONSIDERATO che l'articolazione organizzativa dell'Istituto è così fondata: collaboratori del Dirigente Scolastico, personale docente (compresi docenti esterni ufficialmente incaricati di esami o altre funzioni presso l'Istituto), personale di Segreteria, personale ausiliario (Collaboratori scolastici), personale assistente tecnico e membri (anche esterni alla scuola) degli Organi Collegiali.

DETERMINA

di Designare l'unità organizzativa "Segreteria" comprensiva del Direttore SGA e degli Assistenti Amministrativi ed eventuale personale docente fuori ruolo assegnato, quale autorizzata del trattamento dei dati personali su supporto cartaceo e/o elettronico, ai quali le SS.LL. hanno accesso nell'espletamento delle funzioni e dei compiti assegnati nell'ambito del rapporto di lavoro con questa istituzione scolastica e disciplinati dalla normativa in vigore e dai contratti di settore. In particolare, in qualità di **addetti alla Segreteria amministrativa della scuola** le SS.LL sono incaricate delle operazioni di raccolta, registrazione,

organizzazione, conservazione, consultazione, elaborazione, modifica, selezione, raffronto, estrazione, utilizzo, interconnessione, blocco*, comunicazione*, diffusione*, cancellazione* (*nei soli casi autorizzati dal Titolare del Trattamento), di dati connesse alle seguenti funzioni e attività dalle SS.LL esercitate:

Alunni e genitori
- gestione archivi elettronici e cartacei alunni e genitori;
- consultazione documenti e registri di attestazione dei voti e di documentazione della vita scolastica dello studente, nonché delle relazioni tra scuola e famiglia;
- gestione contributi e/o tasse scolastiche versati da alunni e genitori;
- adempimenti connessi alla corretta gestione degli infortuni;
- adempimenti connessi alle gite scolastiche;
- adempimenti connessi alla vita scolastica degli alunni;

Personale ATA e Docenti
- gestione archivi elettronici e cartacei del Personale ATA e Docenti;
- adempimenti connessi alla vita lavorativa dei dipendenti;

Contabilità e finanza
- gestione archivi elettronici e cartacei della contabilità;
- gestione stipendi e pagamenti, nonché adempimenti di carattere previdenziale;
- gestione rapporti con i fornitori;
- gestione Programma annuale e fondo di istituto
- corretta tenuta dei registri contabili.

Protocollo e archivio corrispondenza ordinaria
- attività di protocollo e archiviazione della corrispondenza ordinaria;
- rapporti con Enti, PA, altre scuole
- rapporti con cittadini

Attività organi collegiali
- gestione degli archivi elettronici e cartacei operazione di consultazione e estrazione dati dai verbali degli organi collegiali.

Si rende noto, a tal fine, che le operazioni sopra descritte vanno rigorosamente effettuate tenendo presenti le istruzioni operative che seguono:

1. il trattamento dei dati personali cui le SS.LL. sono autorizzate ad accedere deve avvenire secondo le modalità definite dalla normativa in vigore, in modo lecito e secondo correttezza e con l'osservanza - in particolare - delle prescrizioni di cui al Regolamento UE 2016/679;
2. il trattamento dei dati personali è consentito soltanto per lo svolgimento delle funzioni istituzionali della scuola;
3. i dati personali, oggetto dei trattamenti, devono essere esatti ed aggiornati, inoltre devono essere pertinenti, completi e non eccedenti le finalità per le quali vengono raccolti e trattati;
4. è vietata qualsiasi forma di diffusione e comunicazione dei dati personali trattati che non sia strettamente funzionale allo svolgimento dei compiti affidati e autorizzata dal titolare del trattamento. Si raccomanda particolare attenzione a tutela del diritto alla riservatezza degli interessati (persone fisiche a cui afferiscono i dati personali);

5. si ricorda che l'obbligo di mantenere la dovuta riservatezza in ordine alle informazioni delle quali si sia venuti a conoscenza nel corso dell'incarico, deve permanere in ogni caso, anche quando sia venuto meno l'incarico stesso;
6. i trattamenti andranno effettuati rispettando le misure di sicurezza predisposte nell'istituzione scolastica; in ogni operazione di trattamento andrà garantita la massima riservatezza e custodia degli atti e dei documenti contenenti dati personali che non andranno mai lasciati incustoditi o a disposizione di terzi non autorizzati ad accedervi, prendervi visione o ad effettuare qualsivoglia trattamento;
7. essere consapevole che le risorse informatiche e telefoniche sono di proprietà della scuola e che devono essere utilizzate per fini strettamente lavorativi, e assolutamente non per scopi diversi né tanto meno per fini personali. Anche la casella di posta ed il collegamento ad Internet devono essere considerati strumenti di lavoro, per cui le persone assegnatarie devono ritenersi responsabili del corretto utilizzo degli stessi e devono essere consapevoli che il Titolare del Trattamento può svolgere dei controlli per garantire sicurezza e funzionalità dei sistemi;
8. le eventuali credenziali di autenticazione (codice di accesso e parola chiave per accedere ai computer e ai servizi web) attribuite alle SS.LL sono personali e devono essere custodite con cura e diligenza; non possono essere messe a disposizione né rivelate a terzi; non possono essere lasciate incustodite, né in libera visione. Si raccomanda la massima attenzione nell'uso delle credenziali di accesso al registro elettronico e ai servizi scolastici abilitati, ricordando che è vietato memorizzarle sui PC ad utilizzo comune, sui dispositivi personali è sconsigliato ed è comunque sotto la propria responsabilità, la password deve avere un minimo di complessità (almeno 10 caratteri alfanumerici fra cui almeno un numero e una lettera maiuscola), va cambiata con una certa frequenza, almeno ogni 90 giorni in presenza di dati particolari (sensibili). In caso di smarrimento e/o furto, bisogna darne immediata notizia al Titolare (o, in caso di assenza al suo sostituto) del trattamento dei dati;
9. si invita il personale ad adottare l'autenticazione a due fattori ove disponibile;
10. sui PC e negli archivi in cloud dell'istituto non devono permanere documenti privati ed in particolare quelli contenenti dati personali;
11. tutti i documenti realizzati con l'ausilio del PC devono di norma esser salvati solo ed esclusivamente nell'archivio elettronico in uso alla scuola (su Server locale e/o in cloud) secondo i criteri di classificazione e archiviazione definiti nel manuale di gestione documentale;
12. nel caso in cui per l'esercizio delle attività sopra descritte sia inevitabile l'uso di supporti rimovibili (quali ad esempio chiavi USB, CD-ROM, ecc), su cui sono memorizzati dati personali, essi vanno custoditi con cura, né messi a disposizione o lasciati al libero accesso di persone non autorizzate;
13. i supporti rimovibili contenenti dati personali e sensibili e/o giudiziari se non utilizzati vanno distrutti o resi inutilizzabili;
14. quando un'intera serie di dati contenuti su supporti esterni deve essere eliminata, si deve formattare il supporto stesso in quanto non è sufficiente la semplice cancellazione dei dati. Per quanto invece concerne i CD-ROM che non sono più necessari, non potendo esser cancellati in alcun modo, devono esser fisicamente distrutti mediante frattura del CD stesso;

15. i documenti contenenti dati personali particolari Art.9 e 10 GDPR (ex sensibili e giudiziari) devono essere protetti in uno dei modi che seguono: protezione del documento tramite password complessa all'apertura, pseudonomizzati, ovvero sostituendo i dati identificativi con dei codici, senza i quali l'interessato non è identificabile. In alternativa salvati su supporti criptati o all'interno di cartelle criptate, o in archivi (cartelle su server o fascicoli in segreteria digitale) a carattere riservato (accessi limitati alle persone autorizzate) come disposto dal titolare;
16. l'invio di dati personali Art.9 e 10 GDPR (ex sensibili e giudiziari) deve avvenire solo se necessario e dove possibile tramite PEC, i file allegati devono essere protetti in uno dei modi che seguono: protezione del documento tramite password complessa all'apertura, pseudonomizzati, ovvero sostituendo i dati identificativi con dei codici, senza i quali l'interessato non è identificabile;
17. l'accesso agli archivi contenenti dati Art.9 e 10 GDPR (ex sensibili e giudiziari) è permesso solo alle persone autorizzate e soggetto a continuo controllo secondo le regole definite dallo scrivente;
18. durante i trattamenti i documenti contenenti dati personali vanno mantenuti in modo tale da non essere alla portata di vista di persone non autorizzate;
19. al termine del trattamento occorre custodire i documenti contenenti dati personali all'interno di archivi/cassetti/ armadi muniti di serratura;
20. i documenti della scuola contenenti dati personali non possono uscire dalla sede scolastica, né copiati, se non dietro espressa autorizzazione del titolare del trattamento;
21. le SS.LL che effettuano l'accesso alle funzioni dei sistemi telematici in uso all'istituzione scolastica (Segreteria Digitale, Registro elettronico, SIDI ..) con i propri dispositivi (PC, notebook, tablet, smartphone ecc.) devono verificare che i medesimi siano conformi alle misure di sicurezza previste dalla normativa, si prendano come riferimento le misure di sicurezza adottate in istituto;
22. l'accesso ai sistemi telematici fuori dall'orario di lavoro e presso sedi diverse da quella scolastica deve essere autorizzato dal titolare del Trattamento, si ricorda che le attività degli utenti sono registrate in un file di log a cui il Titolare in caso di comprovato motivo può averne accesso;
23. in caso di allontanamento anche temporaneo dal posto di lavoro, o comunque dal luogo dove vengono trattati i dati, l'incaricato dovrà verificare che non vi sia possibilità da parte di terzi, anche se dipendenti non incaricati, di accedere a dati personali per i quali era in corso un qualunque tipo di trattamento;
24. le comunicazioni agli interessati (persone fisiche a cui afferiscono i dati personali) dovranno avvenire in forma riservata;
25. all'atto della consegna di documenti contenenti dati personali l'incaricato dovrà assicurarsi dell'identità dell'interessato o di chi è stato delegato al ritiro del documento in forma scritta

26. in caso di comunicazioni elettroniche ad alunni, colleghi, genitori, personale della scuola o altri soggetti coinvolti per finalità istituzionali, queste (comunicazioni) vanno attuate seguendo le indicazioni fornite dall'Istituzione scolastica e avendo presente la necessaria riservatezza delle comunicazioni stesse e dei dati coinvolti.

27. l'installazione di software su dispositivi della scuola deve essere autorizzata dal Dirigente o suo delegato, sentito l'Amministratore di Sistema. Non possono in alcun modo esser caricati, su PC di proprietà della scuola, programmi che non sono stati regolarmente acquistati e dotati di regolare licenza d'uso, nonché esplicitamente autorizzati dal Dirigente. Nel caso non venisse osservata la presente disposizione, l'istituzione scolastica si riserva il diritto di richiedere, a titolo di risarcimento danni, le somme pagate a fronte di: richiesta danni da parte di terzi, multe o sanzioni amministrative comminate da parte della Guardia di Finanza, del Garante per la protezione dei dati, della Polizia Postale o di altre organizzazioni autorizzate. Nel caso in cui il programma non autorizzato abbia causato un malfunzionamento ai sistemi informatici della scuola, saranno addebitati i costi connessi al ripristino della funzionalità dei dispositivi danneggiati.

Di dare atto che:

a) ogni dipendente che cessa di far parte di questa unità organizzativa, cessa automaticamente dalla funzione di Incaricato;
b) che ogni nuovo dipendente che entra a far parte di questa unità organizzativa assume automaticamente la funzione di incaricato;
c) in un determinato momento l'elenco degli incaricati appartenenti a questa categoria corrisponde all'elenco dei dipendenti validamente in servizio che ne fanno parte;

La presente determina è pubblicata sul sito della scuola nella sezione Privacy dove le SS.LL potranno prenderne visione.
Al fine di rendere maggiormente consapevoli e informate le SS.LL, sulle tematiche sopra esposte, saranno organizzate periodicamente attività formative.

Il Dirigente Scolastico
(Dott. Patrizia Galeri)
(firmato digitalmente ai sensi del C.A.D. e s.m.i)