ISTITUTO COMPRENSIVO “DON BOSCO” - ROTONDA (PZ)

SCUOLA DELL’ INFANZIA, PRIMARIA E SECONDARIA DI I GRADO

plesso scolastico ed **uffici** - **via Pietro Nenni – 85048 – ROTONDA (Potenza): *tel.* 0973-661049 - *P. IVA* – 84002200768**

Codice Meccanografico: PZIC828003 - *e-mail:* PZIC828003@istruzione.it

***Posta certificata:* PZIC828003@pec.istruzione.it**

SEZIONE ASSOCIATA CASTELLUCCIO INFERIORE (PZ)

INCARICO GDPR PERSONALE DOCENTE

Al personale docente

Oggetto: designazione incaricato al trattamento dati ex GDPR Regolamento UE 679/2016 e D. Lgs. 101/2018.

IL DIRIGENTE

VISTO il Regolamento UE 2016/679 con particolare riguardo agli artt. 24, 28, 29 e 32;

VISTO il Decreto Legislativo 30 giugno 2003, n. 196 e ss. mm. e ii. (in particolare il D. Lgs. 101(2018), “Codice in materia di protezione dei dati personali”, nel seguito indicato sinteticamente come Codice, ed in particolare gli artt. 28 (titolare del trattamento), 29 (responsabile del trattamento) e 30 (incaricati del trattamento);

CONSIDERATO che questo Istituto è titolare del trattamento dei dati personali di alunni, genitori, personale dipendente, fornitori, e qualunque altro soggetto abbia rapporti con l’Istituto medesimo;

CONSIDERATO che le SS.LL, in servizio presso questo Istituto come docenti (in tale ambito, ai fini del presente incarico, rientrano anche i docenti esterni incaricati ufficialmente di funzioni nella scuola quali ad esempio esami, corsi, e attività integrative) per l’espletamento delle loro funzioni, hanno necessità di trattare dati personali relativi agli alunni di questa Istituzione Scolastica, alle loro famiglie e agli esercenti la funzione genitoriale, fermi restando gli obblighi e le responsabilità civili e penali;

DESIGNA

le SS.LL. quali incaricati del trattamento dei dati personali, su supporto cartaceo o digitale, per l’espletamento delle funzioni e dei compiti connessi al rapporto di lavoro con questa istituzione scolastica e disciplinati dalla normativa in vigore e dai contratti di settore.

In particolare, in qualità di Docenti, le SS.LL sono incaricate delle operazioni di raccolta, registrazione, organizzazione, conservazione, consultazione, modifica, connesse alle seguenti funzioni e attività svolte:

Alunni e genitori

- attività didattica e partecipazione agli organi collegiali;
- valutazione alunni;
- tenuta documenti e registri di attestazione dei voti e di documentazione della vita scolastica dello studente, nonché delle relazioni tra scuola e famiglia quali ad esempio richieste, istanze e corrispondenza con le famiglie;
- rapporti con famiglie e alunni in situazione di disagio psico-sociale; ricezione di documentazione relativa allo stato di salute degli alunni, documentazione alunni diversamente abili, documentazione mensa/intolleranze, documentazione DSA e BES, nei limiti sempre di quanto strettamente necessario;
- eventuali contributi e/o tasse scolastiche versati da alunni e genitori;
- adempimenti connessi alle visite guidate e ai viaggi d'istruzione;
- conoscenza di dati relativi a professioni di fede religiosa;
- eventuali adempimenti connessi al rapporto di pubblico impiego (quali, per es. registrazione presenze, attestazioni inerenti lo stato del personale).

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 delle prescrizioni di cui al Regolamento UE 2016/679 e al Dlgs 101/2018;
2. il trattamento dei dati personali è consentito soltanto per lo svolgimento delle funzioni istituzionali;
3. le eventuali credenziali di autenticazione 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. In caso di smarrimento e/o furto, bisogna darne immediata notizia al titolare del trattamento dei dati;
4. 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;
5. 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 responsabile o dal titolare del trattamento. Si raccomanda particolare attenzione alla tutela del diritto alla riservatezza degli interessati (persone fisiche a cui afferiscono i dati personali);
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;
7. 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;
8. in caso di trattamento su supporto cartaceo, i documenti dovranno essere custoditi in luoghi ad accesso controllato e riservato;
9. i documenti della scuola contenenti dati personali non possono uscire dalla sede scolastica, né copiati, se non dietro espressa autorizzazione del responsabile o dal titolare del trattamento;
10. 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 non autorizzati, di accedere a dati personali per i quali era in corso il trattamento;
11. le comunicazioni agli interessati dovranno avvenire in forma riservata;
12. 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;

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

Si allegano le linee guida specifiche per il personale docente.

IL DIRIGENTE SCOLASTICO

Prof. Nicola Pongitore

Documento firmato digitalmente ai sensi del CAD

E norme ad esso correlate

Linee guida specifiche per il personale docente in presenza

Misure operative per garantire la sicurezza del trattamento dati GDPR Regolamento UE 679/2016

1. Garantire la segretezza delle credenziali riservate per l'accesso al registro elettronico o a qualunque area riservata connesse al proprio incarico. Si rammenta, inoltre, che non è consentito memorizzare tali credenziali nei browser.
2. Consegnare i certificati medici esibiti dagli alunni a giustificazione delle assenze (o qualunque altro documento contenente dati personali o particolari) tempestivamente al collaboratore scolastico, avendo cura che nessuno possa prenderne visione. Il collaboratore scolastico avrà l'obbligo della trasmissione immediata in segreteria.
3. Per i plessi o le sezioni distaccate prive di ufficio di segreteria, la documentazione riservata di cui al punto precedente, dovrà essere consegnata al collaboratore scolastico preposto, che avrà l'obbligo di consegnarli tempestivamente in segreteria.
4. I Piani Didattici Personalizzati e i Piani Educativi Individuali sottoscritti dai docenti e dai genitori, devono essere tempestivamente consegnati in segreteria. Eventuali copie di tali documentazioni devono essere autorizzate dal titolare del trattamento e saranno prive dei dati personali che possano consentire l'individuazione dell'alunno.
5. È vietata, nell'alveo delle funzioni istituzionali, la condivisione e la comunicazione/diffusione di messaggi, foto e immagini riguardanti gli alunni attraverso le APP di messaggistica online (ad es. Whatsapp, Telegram) e sui profili social network personali (ad es. Facebook, Twitter, Instagram). Eventuali comportamenti in difformità di quanto definito sono attivati sotto la piena responsabilità civile e penale del singolo docente.

Nell'uso dei PC e delle dotazioni tecnologiche dell'Istituto è necessario attenersi alle seguenti istruzioni operative:

1. È vietato l'utilizzo di Pen Drive, Hard Disk portatili e ogni altro dispositivo di storage personale, ovvero l'utilizzo di tali dispositivi è condizionato alla predisposizione preventiva degli stessi con tecniche crittografiche;
2. È vietato memorizzare documenti sui PC della scuola;
3. Curare la conservazione e la segretezza delle proprie credenziali di accesso al registro elettronico e ad ogni altra area riservata; Le password impostate devono essere di tipologia "forte", intendendosi una combinazione casuale di lettere (maiuscole e minuscole), numeri, caratteri speciali, in alcun modo riconducibile al titolare dell'account.
4. È vietata la consultazione della propria casella di posta elettronica sui PC della scuola;
5. Nel caso in cui sia necessario accedere ad un proprio account di servizi cloud (ad esempio Google Drive), al termine dell'utilizzo assicurarsi che sia avvenuta la disconnessione dal proprio account.
6. Comunicare tempestivamente al Titolare qualunque anomalia riscontrata nel funzionamento del computer;
7. Spegnere correttamente il computer al termine di ogni sessione di lavoro, evitando di abbandonare la propria postazione di lavoro senza averla spenta.

Linee guida specifiche per il personale docente in DDI, DAD e FAD

Misure operative per garantire la sicurezza del trattamento dati GDPR Regolamento UE 679/2016

Le presenti linee guida forniscono le indicazioni operative per il trattamento di dati personali effettuato al di fuori della sede di lavoro, mediante le modalità di svolgimento della prestazione lavorativa a distanza.

Le prescrizioni sottoriportate dovranno essere attese, se possibile, con ancora più attenzione per garantire un livello di protezione adeguato delle dotazioni tecnologiche attraverso le quali svolge le lezioni a distanza e rispettare i principi di integrità, riservatezza e disponibilità dei dati e delle informazioni ivi contenute, al fine di ridurre al minimo i rischi di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità oppure di distruzione o perdita dei dati stessi.

Pertanto, Lei dovrà rispettare le seguenti direttive

1. L'utilizzo delle dotazioni tecnologiche deve avvenire nel rigoroso rispetto delle linee guida e delle istruzioni fornite dall'Amministrazione.
2. Nell'esecuzione della prestazione lavorativa a distanza, il lavoratore è tenuto al rispetto degli obblighi di riservatezza, ai sensi del decreto del Presidente della Repubblica 16 aprile 2013, n. 62, "Regolamento recante codice di comportamento dei dipendenti pubblici" e ss.mm.ii e dell'art. 13 del CCNL del 18/04/2018.
3. Restano ferme le disposizioni in materia di responsabilità, infrazioni e sanzioni contemplate dalle leggi e dai codici di comportamento sopra richiamati, che trovano integrale applicazione anche al lavoratore agile.
4. Riguardo al trattamento dei dati personali, ovviamente anche fuori sede il dipendente dovrà osservare tutte le istruzioni e le misure di sicurezza previste dalla normativa sulla privacy e riportate nelle linee guida allegate.

In particolare, il docente:

- deve porre ogni cura per evitare che ai dati possano accedere persone non autorizzate presenti nel luogo della prestazione lavorativa fuori sede;
- deve rendere inaccessibile a terzi l'elaboratore in dotazione in caso di allontanamento dalla postazione di lavoro, anche per un intervallo limitato di tempo;
- alla conclusione della prestazione lavorativa giornaliera è obbligatorio custodire, conservare e tutelare i documenti eventualmente stampati provvedendo a distruggerli o a portarli in sede una volta terminato il periodo

Principali prescrizioni in tema di sicurezza informatica

1. Proteggere l'accesso alla rete (LAN, WiFi) e alle dotazioni tecnologiche (PC, notebook, tablet, smartphone, ecc.) attraverso l'uso di password forti e diverse per ciascun servizio[1]. Allo scopo si prescrive il cambio delle password utilizzate abitualmente per l'accesso alle varie applicazioni in cloud. Si consiglia, inoltre, il cambio della password di accesso della propria linea ADSL. Laddove possibile, utilizzare l'autenticazione a due fattori. Ad esempio, gli applicativi Argo consentono l'attivazione del PIN di autenticazione in aggiunta alla password d'accesso. Medesima possibilità è garantita dagli account Microsoft.

[1]La password deve essere sufficientemente lunga e complessa, ad esempio deve essere composta da almeno 8 caratteri, contenere almeno un carattere appartenente alle lettere maiuscole e almeno un carattere appartenente alle lettere minuscole, contenere almeno un carattere appartenente alle 10 cifre (0-9), contenere almeno un carattere appartenente ai caratteri non alfabetici (ad esempio !,$,#,%), essere diversa dall'ultima utilizzata e mai riconducibile alla propria sfera personale o professionale.

2. Garantire che i sistemi operativi installati sulle workstation (PC, notebook, tablet, smartphone) siano autentici e aggiornati all'ultima versione disponibile. Non è consentito lo smart working attraverso workstation dotate di sistemi operativi privi del supporto (ad esempio Windows 7) o peggio non autentici (privi della licenza d'uso). Le vulnerabilità proprie dei sistemi operativi non autentici o privi del supporto e quindi non aggiornati con le ultime patch di sicurezza è la prima causa di accesso non autorizzato alla rete e alle informazioni.

3. Nel caso di utilizzo di una workstation condivisa (PC, notebook, tablet) è obbligatorio implementare un nuovo account d'accesso al sistema, personale e riservato.

4. Garantire la presenza, sulla propria workstation, di un firewall e di un sistema antivirus. Il sistema antivirus deve essere sempre attivo e aggiornato in real time (va bene, ad esempio, anche Avira nella sua versione non commerciale). Il firewall (va bene anche quello integrato nel sistema operativo Windows) deve sempre essere attivo e non deve prevedere alcuna eccezione.

5. È assolutamente vietata la pratica di memorizzazione delle password dei vari account nel browser. È consigliabile evitare di memorizzare anche le user name. Pertanto, il completamento automatico deve essere disabilitato. Si consiglia di utilizzare, per l'accesso ai vari account in cloud, sempre lo stesso browser. La memorizzazione degli account in cloud può essere consentita solo in presenza di un gestore di password crittografico (ad esempio, l'applicazione "Password Manager" integrata nella suite gratuita di Avira).

6. Nel caso in cui si proceda a memorizzare in locale qualsivoglia tipologia di informazioni, anche temporaneamente, le stesse non dovranno mai essere memorizzate sull'hard disk della workstation, ma sempre in un dispositivo rimovibile (ad esempio pen drive, hard disk portatile) protetto su base crittografica. A tal proposito è possibile attivare la funzione "Attiva Bitlocker" fornita dal sistema operativo Windows.