



Ministero dell'Istruzione, dell'Università e della Ricerca
CENTRO PROVINCIALE per L'ISTRUZIONE DEGLI ADULTI
Provincia di Belluno

Via Mur di Cadola, 12 – 32100 BELLUNO – Tel. 0437.31143

e-mail: blmm08400l@istruzione.it - PEC: blmm08400l@pec.istruzione.it

Cod. Mecc.: BLMM08400L – C. F.: 93051950256 - Codice fatturazione elettronica: UFYKUO

**A tutti i Collaboratori scolastici
in servizio presso l'Istituto**

All'Albo

OGGETTO: Collaboratore scolastico autorizzato al trattamento dei dati personali sotto l'autorità diretta del Titolare - art. 4, numero 10 e cons. 29 del RGPD 2016/679

IL DIRIGENTE

1. considerato che l'articolo 4, n. 10 del Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (d'ora in poi «**Regolamento**») – direttamente applicabile dal 25 maggio 2018 in tutta l'Unione europea – introduce la figura ed il ruolo delle “persone autorizzate al trattamento”, ossia le persone fisiche “*autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile*”;
2. considerato che, ai sensi del Regolamento, per «**dato personale**» si intende 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, uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
3. considerato che questo Istituto è Titolare del trattamento (d'ora in poi «**Titolare**») dei dati personali di alunni, genitori, personale dipendente e di qualunque altro soggetto che abbia rapporti con l'Istituto medesimo e che a questo conferisca, volontariamente o per obbligo, propri dati personali o i cui dati siano stati raccolti, sempre e solo per ragioni istituzionali, presso terzi;
4. considerato che l'articolo 29 del Regolamento prescrive che chiunque agisca sotto l'autorità del responsabile (se nominato) o del Titolare del trattamento, che abbia accesso a dati personali, non può trattare tali dati se non è istruito in tal senso dal Titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri;
5. considerato che il Titolare ritiene necessario procedere all'autorizzazione del proprio personale al trattamento dei dati personali nello svolgimento delle proprie mansioni, nonché fornire istruzioni per garantire che la relativa attività sia svolta nel rispetto del Regolamento;
6. considerato che la titolarità del trattamento dei dati personali è esercitata dallo scrivente Dirigente dell'Istituto, in qualità di legale rappresentante dello stesso;
7. considerato che Le SS.LL. in servizio presso questo Istituto come Collaboratori Scolastici per l'espletamento delle Loro funzioni, hanno talvolta anche la necessità di venire a conoscenza e di trattare dati personali, fermi restando gli obblighi e le responsabilità civili e penali;

NOMINA

Le SS.LL. quali

AUTORIZZATI AL TRATTAMENTO DEI DATI PERSONALI

ai sensi dell'art. 29 del Regolamento, in relazione alle operazioni di 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 la scrivente istituzione scolastica e disciplinati dalla normativa in vigore e dai contratti di settore.

In particolare, **in qualità di Collaboratori scolastici dell'Istituto**, alle SS.LL. può essere affidata temporaneamente la custodia, lo spostamento, l'archiviazione o la riproduzione (nell'ambito dei locali dell'istituzione scolastica) di documenti contenenti dati personali, nonché la ricezione di documentazione (quale, ad esempio, richieste di uscite anticipate o domande di iscrizione a scuola) da parte delle famiglie degli alunni o di altre persone.

Le operazioni sopra descritte vanno rigorosamente effettuate tenendo presenti le istruzioni operative che seguono:

1. il trattamento dei dati personali è consentito soltanto per lo svolgimento delle funzioni istituzionali della scuola, per la parte legata al proprio profilo professionale;
2. non possono essere eseguiti trattamenti su ambiti diversi da quelli indicati nel Registro dei Trattamenti della scrivente Istituzione scolastica;
3. i dati devono sempre essere esatti ed aggiornati, se non si ritiene che lo siano e non si ritiene di poter intervenire direttamente occorre segnalarlo prontamente al Titolare del trattamento o a altra persona da lui eventualmente indicata, inoltre, i dati personali devono essere trattati solo se necessario e solo se le attività svolte non possono essere eseguite attraverso il trattamento di semplici dati anonimi;
4. i dati personali particolari (che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona), previsti dall'art.9 Regolamento, nonché i dati relativi a condanne penali o reati, previsti dall'articolo 10 del Regolamento, vanno trattati solo nei casi strettamente indispensabili (in caso di dubbi rivolgersi al Titolare o a altra persona da lui eventualmente indicata), nel rispetto delle prescrizioni di legge o di regolamento e nei limiti indicati dal D.M 305/2006 (Regolamento recante identificazione dei dati sensibili e giudiziari trattati e delle relative operazioni effettuate dal Ministero della pubblica istruzione) e dagli atti autorizzatorii, prescrittivi e normativi che in futuro sostituiranno tale Decreto;
5. nell'accedere alle banche dati ed agli archivi cartacei della scuola e ai documenti correlati, contenenti i dati personali, occorre rispettare i principi fondamentali sanciti dall'art. 5 del Regolamento, garantendo sempre la riservatezza degli stessi dati;
6. non è possibile realizzare, senza la preventiva autorizzazione del Titolare, nuove ed autonome basi dati, in ossequio al principio di minimizzazione dei trattamenti;
7. occorre rispettare ogni misura di sicurezza adottata dal Titolare, ivi incluso il rispetto delle procedure interne in materia di utilizzo delle strumentazioni informatiche e delle credenziali di autenticazione, di custodia di atti e documenti affidati, che non andranno mai lasciati incustoditi o a disposizione di terzi non autorizzati ad accedervi o a prendervi visione o a altro trattamento;
8. eventuali credenziali di autenticazione (ad esempio, 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. In caso di smarrimento e/o furto, bisogna darne immediata notizia al Titolare o a altra persona da lui eventualmente indicata;
9. 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, devono prevedere forme di sicurezza (criptazione) e non devono essere messi a disposizione o lasciati al libero accesso di persone non autorizzate;
10. si ricorda, inoltre, che l'accesso agli archivi (cartacei e digitali) della scuola e ai locali di segreteria è permesso solo alle persone autorizzate ed è soggetto a continuo controllo secondo le regole definite dallo scrivente;
11. durante i trattamenti, i documenti contenenti dati personali vanno mantenuti in modo tale da non essere alla portata di vista di persone non autorizzate;
12. al termine del trattamento occorre custodire i documenti contenenti dati personali all'interno di archivi/cassetti/armadi indicati dal Titolare secondo le regole interne;

13. 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 degli stessi trattamenti, di accedere a dati personali per i quali era in corso un qualunque tipo di trattamento, sia cartaceo che automatizzato;
14. in caso di comunicazioni elettroniche 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;
15. non bisogna mai comunicare i dati personali trattati in ragione del proprio lavoro all'esterno, salvo che tale comunicazione sia necessaria per l'esecuzione del proprio lavoro e che si sia certi che le persone esterne siano autorizzate a conoscere le informazioni; è vietata qualsiasi forma di diffusione (anche attraverso il sito web della scuola) e comunicazione dei dati personali trattati, fatti salvi i casi esplicitamente previsti da norme di legge e di regolamento;
16. bisogna prestare la massima attenzione al trattamento di foto e video, se si hanno dubbi sulla legittimità del trattamento occorre rivolgersi al Titolare o a altra persona da lui eventualmente indicata;
17. i documenti della scuola contenenti dati personali non possono essere portati fuori dalla sede scolastica, né copiati, se non dietro espressa autorizzazione del Titolare del trattamento o di altra persona da lui eventualmente indicata. Gli stessi principi valgono per Personal Computer o altri strumenti elettronici in uso presso la scuola, contenenti dati personali;
18. le comunicazioni agli interessati (persone fisiche a cui afferiscono i dati personali) dovranno avvenire in forma riservata;
19. all'atto della consegna di documenti contenenti dati personali l'autorizzato al trattamento dovrà assicurarsi dell'identità dell'interessato o di chi è stato delegato al ritiro del documento in forma scritta;
20. occorre comunicare al Titolare del Trattamento o a altra persona da lui eventualmente indicata qualunque notizia sia ritenuta rilevante con riferimento al trattamento dei dati personali, con particolare riguardo a eventuali violazioni di dati personali, o presunte tali, a perdite di dati o ad eventuali richieste dei soggetti interessati aventi ad oggetto l'esercizio dei loro diritti come previsti dal Regolamento (accesso, cancellazione, modifica, rettifica, ecc.);
21. in caso di eventuali dubbi o notizie che si reputino rilevanti con riferimento al trattamento dei dati personali, occorre rivolgersi al Titolare o a altra persona da lui eventualmente indicata;
22. è fondamentale, anche in chiave di responsabilità personale, partecipare ai corsi di formazione in materia privacy organizzati dal Titolare.

= = =

Ad ulteriore esemplificazione operativa dell'ordinaria diligenza richiesta ai punti da 1 a 22, che precedono,

IN PARTICOLARE SI RACCOMANDANO LE SEGUENTI CAUTELE STANDARD:

SCRIVANIA PULITA

I supporti cartacei e quelli informatici mobili di cui il Collaboratore scolastico abbia la disponibilità, quando non sono presidiati per periodi di tempo significativi, devono essere sistemati in armadi adeguatamente chiusi o in altri contenitori fisicamente protetti. Le informazioni riservate su carta o supporto informatico, devono essere messe sotto chiave. Per le informazioni strettamente riservate ricorrere, se possibile, a una cassaforte o un armadio blindato e ignifugo in cui riporre quando non sono utilizzate, e in particolare quando nella postazione non c'è nessuno.

VIDEATA PULITA

Per quanto riguarda i PC fissi eventualmente in uso al Collaboratore scolastico, non devono essere lasciati incustoditi con sessioni applicative aperte o con login effettuato, ma devono essere protetti da chiavi fisiche, password o altri tipi di blocchi/controlli (come ad es. screen saver opportunamente programmati).

GESTIONE DELLE PASSWORD

Per la password di accesso alla eventuale postazione informatica di lavoro è necessario attenersi alle seguenti norme:

- deve essere custodita con la massima cura;
- non deve essere comunicata ad altri;

- non deve essere scritta su supporti facilmente accessibili (post-it, blocco appunti, ecc.). Nel caso si voglia mantenerne traccia scritta, per propria memoria, questa deve essere conservata in luogo sicuro;
- deve essere cambiata almeno ogni 3 mesi per i dati sensibili, ogni 6 mesi per i dati comuni;
- deve avere una lunghezza minima di 8 caratteri;
- deve essere formata dalla combinazione di caratteri alfabetici e numerici e contenere almeno una lettera ed un numero;
- non utilizzare più di due caratteri consecutivi identici (es: aaaaa...);
- non utilizzare sequenze di cifre consecutive (es: 12345...);
- non deve essere legata al nome dell'utente, oppure alla sua User-id, o in generale a parole a lui riconducibili (nome della moglie o dei figli, luogo e data di nascita);
- non deve essere basata su parole di uso comune (nomi di luoghi, personaggi, mesi, giorni della settimana, ecc.);
- non deve essere uguale ad una delle ultime 5 già utilizzate;
- non va confidata a nessuno per nessun motivo.

GESTIONE DEI PIN

Per quanto riguarda la gestione dei PIN di smart card o di account di accesso a piattaforme è necessario attenersi alle seguenti norme.

Sia il PIN Utente che la password devono:

- non essere uguali ad una parola presente su un vocabolario, anche se scritta al contrario;
- non essere formati da caratteri continui sulla tastiera (12345678 è un PIN poco sicuro);
- non essere un numero, parola o nome riconducibile alla propria vita (la data di nascita della moglie, il nome del cane, il numero di conto corrente, il numero di passaporto sono password poco sicure);
- non devono essere scritti su supporti facilmente accessibili (post-it, blocco appunti, ecc.). Nel caso si voglia mantenerne traccia scritta, per propria memoria, essa deve essere conservata in luogo sicuro;
- non vanno confidati a nessuno per nessun motivo.

USO DEGLI ARMADI BLINDATI

Per l'uso degli armadi blindati e delle relative chiavi, l'incaricato dovrà applicare scrupolosamente le regole e le procedure espressamente definite dal Titolare o dal Responsabile interno del trattamento.

= = =

La presente designazione, relativamente all'autorizzazione ai trattamenti e con le connesse funzioni di responsabilità, ha validità sino alla cessazione del rapporto di lavoro con il singolo Soggetto Autorizzato.

Anche dopo la cessazione del rapporto permangono gli obblighi di riservatezza, di non diffusione, di non comunicazione a soggetti che non siano autorizzati al trattamento.

La presente ha validità permanente, salvo sostituzione con provvedimento espresso. La presente è pubblicata nella sezione "Privacy" del sito di Istituto (<https://www.cpiabl.edu.it/policy-privacy/>) unitamente alle Informativa rese a studenti e famiglie, al personale dipendente e ai fornitori.

Il Dirigente scolastico reggente

Gianni Maddalon

(firma autografa sostituita a mezzo stampa, ai sensi del C.A.D. e norme connesse)

Data _____ Firma del soggetto incaricato _____