ISTITUTO COMPRENSIVO di SERINA
Via Palma il Vecchio ,48 -24017 SERINA (BG)
Cod. Scuola: BGIC87400A - Cod.Fiscale: 85003170165
Telefono: 0345 66067 - **FAX:** 0345 66117
PEC: bgic87400a@pec.istruzione.it - **PEO:** bgic87400a@istruzione.it

Codice deontologico
Norme di comportamento per gli incaricati al trattamento dei dati

Premesso che:

- l'Amministrazione é tenuta a garantire i suoi interlocutori da qualsiasi indebita intrusione della loro sfera di riservatezza e a rispettare, nello svolgimento delle sue funzioni, la disciplina a tutela dei dati personali;
- in ragione di ciò, l'Amministrazione si conforma al principio di necessità, di pertinenza e non eccessività e di rispetto delle finalità del trattamento dei dati, come prescritto dal GDPR n. 679/16 e dal d.lgs. 196/03, cosi come integrato dal D.lgs. 101/18.

Ciò premesso:

- l'Amministrazione fornisce agli incaricati del trattamento le istruzioni per trattare i dati personali nel rispetto di tali principi.

Istruzioni generali

L'incaricato del trattamento é tenuto a:

1. custodire i dati raccolti con la massima diligenza, escludendo dall'accesso tutti coloro che non sono autorizzati;
2. al momento della raccolta dei dati personali, fornire all'interessato l'informativa secondo i modelli predisposti e resi disponibili. Qualora tali modelli non fossero disponibili o dovessero essere aggiornati, l'incaricato é tenuto ad informare di ciò il suo diretto superiore;
3. periodicamente e secondo le disposizioni impartite dal Titolare del trattamento, cancellare i dati personali per i quali non sussistano ragioni di fatto o di diritto che ne giustificano la conservazione;
4. riferire al diretto superiore di eventuali istanze di accesso che comportino la conoscenza di dati personali, prima di provvedere;
5. riferire al diretto superiore di ogni eventuale comunicazione, diffusione ed in genere di ogni trattamento di cui fosse richiesto, non previsto nell'incarico ricevuto.

Istruzioni per i trattamenti automatizzati

L'incaricato é tenuto a:

1. custodire con la massima diligenza le credenziali di autenticazione (user-id e password) per l'utilizzo del computer e per l'accesso alle banche dati e ai sistemi informativi di competenza;
2. mantenere riservata la propria password evitando qualsiasi forma di condivisione;
3. modificare la password almeno ogni sei mesi. Nel caso in cui la password dia l'accesso a dati personali sensibili o giudiziari, essa deve essere modificata almeno ogni tre mesi. La password deve essere composta da almeno 8 caratteri (nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito) e non deve contenere riferimenti facilmente riconducibili all'incaricato;
4. presenziare, quando possibile, agli interventi di assistenza e digitare personalmente la propria password. Qualora ciò non sia possibile, provvedere alla modifica alla password immediatamente dopo l'intervento;
5. utilizzare esclusivamente software reso disponibile da _____;
6. non collegare modem o dispositivi che consentano un accesso non controllato al computer e alla rete di _____;
7. effettuare un back up settimanale dei dati personali residenti sul proprio computer e conservare i supporti removibili in arredi dotati di serratura;

8. non rimuovere l'antivirus installato sul computer e, se necessario, attivare giornalmente la procedura di aggiornamento disponibile via rete;
9. non utilizzare supporti removibili di provenienza esterna e, qualora ciò si rivelasse necessario, verificare sempre preliminarmente l'integrità dei supporti con il programma antivirus installato;
10. non scaricare file eseguibili o documenti di testo da siti internet senza verificare l'assenza di virus;
11. non disabilitare la password di screen saver, per evitare accessi non autorizzati quando la postazione non é presidiata;
12. non condividere il proprio hard disk con un altro computer se non in condizioni di protezione da scrittura e con password di accesso;
13. non riutilizzare supporti removibili sui quali siano conservati dati sensibili o giudiziari a meno che i dati in essi contenuti non siano intelleggibili e tecnicamente ricostruibili. Diversamente, i supporti removibili debbono essere distrutti;
14. qualora dati “sensibili o giudiziari” ai sensi dell’artt. 9 e 10 del GDPR siano registrati in banche dati gestite in locale, adottare tecniche di cifratura a protezione degli stessi;

Istruzioni per i trattamenti cartacei

L'incaricato é tenuto a:

1. custodire gli atti e i documenti contenenti dati personali in armadi muniti di serratura. Qualora gli stessi non fossero disponibili o non fossero sufficienti, l'incaricato é tenuto ad informare di ciò il suo diretto superiore. Nel caso gli atti e documenti contengano dati sensibili o giudiziari, l'accesso agli armadi fuori degli orari d'ufficio dovrà essere registrato in apposito registro;
2. conservare con cura gli atti e documenti contenenti dati personali restituendoli, quando necessario, all'archivio al termine delle operazioni senza trattenerne copia se non strettamente necessario;
3. qualora si trattino dati “sensibili e giudiziari”, verificare insieme al diretto superiore l'opportunità di ricorrere ad archivi separati per la conservazione di tali dati.

Istruzioni per i trattamenti in regime di Lavoro Agile

L’Incaricato è tenuto a:

1. Assicurarsi di non effettuare forme di salvataggio dati di pertinenza dell’istituto sui propri device;
2. Gestire il proprio lavoro mediante accesso a piattaforme (es. segreteria digitale) e soluzioni di Cloud attivate, evitando l’uso di altre soluzioni di terze parti non espressamente autorizzate dall’Istituto;
3. Limitare l’utilizzo del dispositivo al solo incaricato, evitando durante le attività lavorative la condivisione del terminale con altri soggetti non espressamente autorizzati;
4. Prediligere la navigazione in incognito, al fine di garantire riservatezza qualora il dispositivo fosse soggetto ad uso promiscuo;
5. Su richiesta dell’Istituto è possibile installare software per il “Desktop Remote control” ovvero effettuare accesso ad una VPN;
6. Mantenere attiva l’opzione di aggiornamento automatico del S.O. in uso (Windows, Linux, macOS);
7. Installare un software di protezione antivirus, qualora non fosse già presente, al fine di tutelarsi da potenziali attacchi informatici;
8. Utilizzare sempre e solo indirizzi email con dominio istituzionale, evitando email personali non autorizzate;
9. Predisporre la cifratura dei file (inserimento password) quando la stessa si rende necessaria in ragione della natura dei dati trattati (es. documenti contenenti informazioni particolari dell’utenza come stati di salute ecc…);

Serina, 01/09/2020

Il Dirigente Scolastico
Prof. Ghilardi Claudio
Firma autografa omessa ai sensi dell’art. 3 del D.Lgs. n. 39/1993