ISTITUTO COMPRENSIVO DI MAJANO e FORGARIA
SCUOLE DELL'INFANZIA, PRIMARIA E SECONDARIA DI 1° GRADO
Comuni di Majano e Forgaria nel Friuli
Viale G. Schiratti,1 - 33030 MAJANO (UD)
tel. 0432959020 - fax 0432948208 - C.F. 80015380308
web: www.majanoscuole.it - e-mail: udic81500t@istruzione.it
pec: udic81500t@pec.istruzione.it

Prot.n.

Majano, 19 maggio 2021

Ai Docenti dell'IC Majano e Forgaria
Al Personale ATA

OGGETTO: CORRETTA GESTIONE DELLA PRIVACY NEI LUOGHI DI LAVORO

Regole di comportamento per una corretta gestione della privacy nei luoghi di lavoro

Vengono di seguito indicate le misure operative da adottare per garantire la sicurezza dei dati personali e, in particolare, dei dati sensibili e giudiziari:

1. Non comunicare a nessun soggetto non specificatamente autorizzato i dati personali comuni, sensibili, giudiziari, sanitari e/o altri dati, elementi, informazioni dei quali venite a conoscenza nell'esercizio delle vostre funzioni. In caso di dubbio accertarsi sempre dal Titolare del trattamento se il soggetto cui devono essere comunicati i dati sia o meno autorizzato a riceverli.
2. *Chiudere a chiave cassetti ed aule ove possibile.* Il primo livello di protezione di qualunque sistema è quello fisico. E' certamente vero che una porta o un cassetto chiusi possono in molti casi non costituire una protezione sufficiente, ma è anche vero che pone se non altro un primo ostacolo, e richiede comunque uno sforzo volontario non banale per la sua rimozione. Pertanto chiudete i documenti a chiave nei cassetti o negli altri contenitori messi a disposizione ogni volta che potete.
3. Nelle attività di trattamento dei dati (compresa la documentazione contenente dati personali), porre in essere e osservare i seguenti accorgimenti:
   - non far uscire documenti dalla sede scolastica, neanche temporaneamente, salvo ciò non sia assolutamente necessario per l'espletamento dell'incarico e vi sia l'autorizzazione del D.S.;
   - non fare copie della documentazione salvo autorizzazione del D.S./D.S.G.A.;
   - durante il trattamento mantenere i documenti contenenti dati personali lontani dalla vista di terzi estranei;
   - al termine del trattamento custodire i documenti all'interno di archivi muniti di serratura o comunque protetti da accessi indebiti;
   - 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 è in corso un qualunque tipo di trattamento.
4. Custodire in apposito armadio o contenitore dotato di serratura nella stanza individuata come sala professori dell'edificio i seguenti documenti: certificati medici esibiti dagli alunni a giustificazione delle assenze, qualunque altro documento contenente dati personali e/o sensibili degli alunni.
5. *Spegnere il computer se ci si assenta per un periodo di tempo lungo.* Lasciare un computer acceso non crea problemi al suo funzionamento ed al contrario velocizza il successivo accesso. Tuttavia, un computer acceso è in linea di principio maggiormente attaccabile perché raggiungibile tramite la rete o direttamente sulla postazione di lavoro. Inoltre, più lungo è il periodo di assenza maggiore è la probabilità che un'interruzione dell'energia elettrica possa portare un danno.

6. *Non lasciare lavori incompiuti sullo schermo.* Chiudete sempre le applicazioni con cui state lavorando quando vi allontanate dal posto di lavoro per più di pochi minuti: potreste rimanere lontani più del previsto, e un documento presente sullo schermo è vulnerabile (quasi) quanto uno stampato o copiato su dischetto.

7. *REGISTRO ELETTRONICO.* Non salvate le vostre credenziali di accesso al registro elettronico sul PC che trovate nelle aule e ricordate di disconnettervi sempre (cd. log out) al termine del vostro orario di lezione. Il mancato rispetto di questi accorgimenti potrebbe consentire ad un utente di effettuare modifiche o alterazioni ai dati personali presenti all'interno del registro medesimo e la traccia informatica corrisponderebbe alle vostre credenziali. Ricordatevi pertanto di rispettare scrupolosamente la presente regola.

8. *Proteggere attentamente i dati.* Bisogna prestare particolare attenzione ai dati importanti di cui si è personalmente responsabili. Poiché può risultare difficile distinguere tra dati normali e dati importanti, è buona norma trattare tutti i dati come se fossero importanti. Come minimo posizionarli in un'area protetta da password e non dare automaticamente a nessun altro utente il permesso di lettura o modifica. Ai dati da condividere applicare i permessi opportuni solo per il tempo strettamente necessario all'interazione con gli altri utenti.

9. Gli insegnanti e gli allievi che utilizzano i computer messi a disposizione dalla scuola per redigere documenti a scopo personale o didattico, devono eliminare la bozza dalla macchina successivamente alla stampa, al salvataggio su diverso supporto o all'invio telematico. Si ricorda poi che è importante non salvare password e/o codici di accesso nei computer condivisi.

10. *Prestate attenzione alle fotocopie*: fare fotocopie di documenti contenenti dati personali sensibili solo se strettamente necessario. Assicurarsi di non lasciare copie nella macchina e se necessario eliminare copie mal riuscite utilizzate una macchina distruggi-documenti (shredder) o stracciate i documenti a mano.

11. *Prestare particolare attenzione all'utilizzo dei computer portatili.* I PC portatili sono un facile bersaglio per i ladri. Se avete necessità di gestire dati riservati su un portatile, proteggetelo con una password, fate installare un programma di cifratura del disco rigido (per impedire la lettura dei dati in caso di furto) ed effettuate periodicamente il backup dei dati.

12. *Proteggere il proprio computer con una password. Abilitare ove possibile l'accesso tramite password.* La maggior parte dei computer offre la possibilità di impostare una password all'accensione. Anche alcuni applicativi permettono di proteggere i propri dati tramite password. Imparate a utilizzare queste caratteristiche che offrono un buon livello di riservatezza.

13. *Fare attenzione a non essere spiati mentre si digita una password o qualunque codice di accesso.* Anche se molti programmi non ripetono in chiaro la password sullo schermo, quando digitate una password questa potrebbe essere letta guardando i tasti che state battendo, anche se avete buone capacità di dattiloscrittura. Chiedete agli astanti di guardare da un'altra parte quando introducete una password o controllate che nessuno stia guardando.

14. *Non permettere l'uso del proprio account ad altri colleghi.* Non comunicate la vostra password di accesso al PC o la password di accesso a software o piattaforme telematiche a nessuno, né tantomeno a colleghi di ufficio. Un'attività illecita svolta da un vostro collega con la vostra Password sarà attribuita a Voi, con tutte le conseguenza giuridiche del caso.

15. *Applicare con cura le linee guida per la prevenzione da infezioni da virus.* La prevenzione dalle infezioni da virus sul vostro computer è molto più facile e comporta uno spreco di tempo molto minore rispetto alla correzione degli effetti di un virus. Inoltre, se non avete attivato adeguate misure antivirus potreste incorrere in una perdita irreparabile di dati o in un blocco anche molto prolungato della vostra postazione di lavoro. A tal fine, è opportuno che in ogni macchina collegata ad internet vi sia installato un programma antivirus e che tale programma sia aggiornato periodicamente.

16. *Tutta la documentazione relativa agli allievi portatori di handicap/certificati/BES va consegnata direttamente al Dirigente Scolastico oppure ad altro soggetto appositamente incaricato.* Per tutto il tempo in cui ne è in possesso il docente è responsabile della custodia e conservazione di tutta la documentazione da egli stesso prodotta o pervenutagli per lo svolgimento delle sue mansioni.

17. La strumentazione intesa come insieme di hardware e software messa a disposizione degli utenti deve essere utilizzata in modo conforme ed esclusivamente per lo svolgimento delle attività professionali cui ogni incaricato è preposto: la strumentazione non deve essere utilizzata per scopi personali.

18. Ugualmente è fatto divieto all'utente di installare programmi non autorizzati. Oltre alla possibilità di trasferire involontariamente un virus o di introdurre un cosiddetto "cavallo di troia", va ricordato che la maggior parte dei programmi sono protetti da copyright, per cui la loro installazione può essere illegale. E' vietato scaricare per qualsiasi finalità, anche connesse con l'attività lavorativa, programmi reperiti in rete (internet) o da qualunque altra sorgente esterna salvo espressa autorizzazione del titolare. Egli,

peraltro, ricorda all'utilizzatore che costituiscono illecito penale le condotte consistenti nell'illecita duplicazione o riproduzione di software ai sensi della legge sul diritto d'autore n. 633/41 e s.m..

19. Particolare attenzione deve essere prestata nei confronti dei supporti rimovibili contenenti dati sensibili o giudiziari: al termine delle operazioni, se non dedicati alla memorizzazione, questi devono essere distrutti o resi inutilizzabili, oppure possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, solo se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.

20. E' vietato configurare l'email istituzionale su applicativi di gestione della posta elettronica installati su dispositivi fissi e mobili privati ed è parimenti vietato memorizzare all'interno dei dispositivi personali le credenziali di accesso agli strumenti di lavoro della scuola.

21. Prestare la massima attenzione in fase di invio di email ad una pluralità di soggetti, avendo cura di evitare che gli indirizzi utilizzati siano visibili a tutti i destinatari. Si ricorda, infatti, che l'invio massivo di un messaggio con gli indirizzi dei destinatari in chiaro, costituisce ai sensi della normativa una divulgazione indebita di dati personali.

22. E' fatto divieto agli utenti di navigare in siti non attinenti l'attività lavorativa, in quanto l'utilizzo del collegamento ad internet deve essere funzionale ad essa e non effettuato per ragioni personali.

23. L'utente non deve utilizzare apparecchiature non consentite o per cui egli non è autorizzato. In particolare, l'utilizzo di modem e di collegamenti wireless non criptati su postazioni di lavoro collegate alla rete di ufficio offre una porta d'accesso dall'esterno non solo al computer dell'utente ma a tutta la rete di cui esso fa parte, con ripercussioni negative sulla sicurezza dell'intera rete. E' quindi vietato l'uso di modem e di collegamenti wireless non criptati all'interno della rete locale.

24. E' fatto divieto di utilizzare, sui sistemi informatici dell'Ente, dispositivi esterni per finalità diverse dalle attività di interesse e pertinenza dell'Ente stesso.

25. E' fatto divieto di collegare alla rete informatica dell'Ente qualsiasi dispositivo personale (PC, smartphone, tablet, stampanti, scanner, chiavette USB personali).

26. L'utente deve utilizzare la posta elettronica in modo appropriato e consapevole:

    A. Non deve rispondere a messaggi indesiderati (spam) e non deve partecipare alle cosiddette "catene di Sant'Antonio", per non dare conferma (implicita) della validità dell'indirizzo di posta.
    B. Deve prestare attenzione al fenomeno del ***phishing***, ossia una tecnica utilizzata per ottenere l'accesso ad informazioni personali e riservate con la finalità del furto di identità mediante l'utilizzo di messaggi di posta elettronica fasulli, opportunamente creati per apparire autentici (ad esempio e-mail artatamente contraffatte per sembrare comunicazioni ufficiali di Istituti Bancari, siti istituzionali, ecc.). Con tali messaggi viene richiesto l'accesso a siti web, all'interno dei quali il mittente (che tenta la truffa) impersona una azienda/ente che chiede al destinatario di inserire i suoi dati di accesso a scopo di verifica, in modo da carpirli ed utilizzarli successivamente in modo fraudolento. La pagina web a cui si è inviati dal link indicato dal mittente della e-mail è identica a quella dell'azienda ma non è realmente quella corretta. In tal modo, se non si presta attenzione all'indirizzo indicato nel browser internet, si è portati a credere, a colpo d'occhio, di essere realmente nella pagina web corretta. In realtà si sta utilizzando una pagina web costruita ad hoc per scopi fraudolenti. Grazie a questi messaggi, l'utente è ingannato e portato a rivelare dati importanti, come numero di conto corrente, nome utente e password, numero di carta di credito ecc.
    C. Stare molto attenti ad aprire documenti allegati alle e-mail apparentemente provenienti da fonti sicure (ad esempio Agenzia Entrate, Enel, Tribunali, o anche da colleghi di lavoro) oppure a cliccare i link (o collegamenti ipertestuali) contenuti nelle predette mail. C'è il rischio infatti che il computer e la rete informatica possano venire infettati da **virus** molto pericolosi (ad es. il *cryptolocker* della famiglia dei cd. *ransomware*) che criptano tutti i dati con la richiesta di un vero e proprio riscatto per ottenere la disponibilità degli stessi. Per riconoscere se il mittente è veramente quello che sembra è sufficiente leggere bene l'indirizzo di provenienza (verificare quindi eventuali errori di battitura o nomi apparentemente sospetti), oppure passando il cursore del mouse sopra l'indirizzo e-mail (comparirà l'indirizzo esatto). Si ricorda infatti

che è molto facile camuffare o celare L'indirizzo del mittente per confondere il destinatario.

27. A questo INDIRIZZO[1] è possibile consultare una guida utile per la prevenzione dai rischi ***ransomware***. Se avete dei dubbi consultate il titolare prima di procedere.

28. La dotazione hardware e software è quindi quella configurata su ciascuna macchina a cura del titolare: ogni modifica deve essergli preventivamente richiesta e da lui autorizzata.

29. Controllate se nella barra degli indirizzi del browser di navigazione (Google Chrome, Mozilla Firefox, Microsoft Edge) il protocollo di navigazione è http oppure https (oppure se compare l'icona di un lucchetto). La presenza dell'icona e/o della scritta https assicura che i dati oggetto di trasmissione sono cifrati e quindi non intelligibili. Ciò è molto importante quando attraverso quel sito web si stanno per trasmettere dati importanti o delicati (ad es. per un pagamento on line con carta di credito).

30. Non comunicate alla stampa giornalistica e/o televisiva notizie, fatti, informazioni di cui venite a conoscenza nello svolgimento della vostra attività lavorativa presso il titolare.

31. *AVVISATE IL D.S. E IL RESPONSABILE DELLA PROTEZIONE DEI DATI SE RITENETE CHE I DATI SIANO STATI VIOLATI*. Allertate immediatamente il D.S. in caso di perdita o distruzione, anche accidentali, di dati personali, e in generale in tutti i caso in cui l'incaricato ragionevolmente ritenga che vi possa essere stata una violazione degli stessi (accessi indebiti, accessi non autorizzati, sottrazione o perdita di password e/o codici di accesso, ecc.).

32. Segnalare al Titolare del trattamento eventuali anomalie o guasti nei sistemi di chiusura degli armadi o dei contenitori adibiti ad archivio.

Per ogni ulteriore informazione sulle modalità di comportamento da tenere sul luogo di lavoro e' necessario far riferimento al dirigente scolastico.

IL DIRIGENTE SCOLASTICO
Francesco Candido

Firma autografa sostituita a mezzo stampa digitale ai sensi dell'art. 3 D.to Lgs 12.02.1993, n. 39