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

Al Personale ATA – AA
Al Sito

OGGETTO: Mansionario ATA – AA - REGOLE DI COMPORTAMENTO per una corretta gestione della PRIVACY nei luoghi di lavoro

MANSIONARIO ATA

REGOLE DI COMPORTAMENTO PER UNA CORRETTA GESTIONE DELLA PRIVACY NEI LUOGHI DI LAVORO

AGGIORNAMENTO N° 1-2020

NORMATIVA DI RIFERIMENTO:

REGOLAMENTO EUROPEO 679/2016.

D.LGS. 196/2003.

CIRCOLARE AGID 18 APRILE 2017 N.2 "MISURE MINIME DI SICUREZZA ICT PER LE PUBBLICHE AMMINISTRAZIONI)

TERMINI E DEFINIZIONI UTILI

DATO PERSONALE	Art. 4, Co. 1: "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 o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;"	Quindi anche: ▪ il Codice Fiscale, la Partita Iva; ▪ i suoni, in caso di registrazione di voci di persone; ▪ le immagini, video/fotoriprese; ▪ i numeri delle utenze telefoniche fisse e mobili; ▪ gli indirizzi e-mail; I dati di identificazione generali, anche indirettamente, della persona (es. le generalità - nome e cognome, indirizzo) sono da considerarsi dati personali "comuni".
DATO IDENTIFICATIVO	i dati personali che permettono l'identificazione diretta dell'interessato;	Il regolamento richiede che l'utilizzo di dati identificativi avvenga solo se necessario al perseguimento degli scopi del trattamento.
DATO ANONIMO	il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;	Non è dato anonimo il dato che viene criptato, poiché il sistema adottato ne consente la decriptazione e quindi l'identificazione

DATO SENSIBILE	*Art. 9, Co. 1* I dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché i 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	I dati sensibili possono essere trattati solo previo consenso dell'interessato o negli altri casi tassativi dell'art. 9. Con i dati giudiziari costituiscono il "nocciolo duro" della privacy, pertanto godono di una tutela maggiore e in quanto tali vanno custoditi e controllati con particolare attenzione. Nel Regolamento formalmente non è presente la definizione di dato sensibile, sostituita con quella di "categorie particolari di dati personali". Esempio: i documenti e certificati medico-sanitari, i documenti da cui si evince l'origine razziale o etnica, la devoluzione dell'8 per mille, le trattenute sindacali in busta paga, il casellario giudiziale, l'appartenenza a categorie di lavoro protette, il certificato di inidoneità al lavoro, le opinioni politiche o filosofiche, componenti biometriche (impronta digitale) a fini identificativi o di autenticazione, ecc.
DATO GIUDIZIARIO	Art. 10: "Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'art. 6, co. 1, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati".	La definizione è più generica rispetto al D.Lgs. 196/2003, ma riguarda sempre i dati inerenti il procedimento penale e non civile. Il loro trattamento è consentito su base legislativa nazionale o comunitaria (ad es. le Autorizzazioni Generali del Garante).
VIOLAZIONE DEI DATI PERSONALI	La violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.	
TITOLARE DEL TRATTAMENTO	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali. Il titolare del trattamento è l'Istituto Scolastico rappresentato dal D.S. in carica *pro tempore*.	
RESPONSABILE DEL TRATTAMENTO	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo interno o esterno che tratta dati personali per conto del titolare del trattamento. E' nominato con atto scritto e si attiene alle istruzioni ricevute dal titolare.	
INCARICATO DEL TRATTAMENTO	Anche se la definizione non è più presente nel nuovo testo regolamentare, si intende ancora la persona fisica o l'unità organizzativa autorizzata o istruita dal titolare o dal responsabile a compiere operazioni di trattamento sui dati personali.	
INTERESSATO	È il soggetto, persona fisica, cui si riferiscono i dati personali, cui sono riconosciuti i diritti di cui agli artt. 15 e seguenti del Regolamento. Per l'Istituto sono da considerarsi interessati: gli allievi; i dipendenti/collaboratori, i fornitori di beni e servizi, gli utenti del sito web istituzionale.	
RESPONSABILE DELLA PROTEZIONE DEI DATI	Il responsabile della protezione dei dati personali (anche conosciuto con la dizione in lingua inglese data protection officer – DPO) è una figura prevista dall'art. 37 del Regolamento (UE) 2016/679. Si tratta di un soggetto designato dal Titolare per assolvere a funzioni di supporto e controllo, consultive, formative e informative relativamente all'applicazione del Regolamento medesimo. Coopera con l'Autorità (e proprio per questo, il suo nominativo va comunicato al Garante) e costituisce il punto di contatto, anche rispetto agli interessati, per le questioni connesse al trattamento dei dati personali (artt. 38 e 39 del Regolamento). L'Ente ha designato come DPO l'Avv. Stefano Corsini, contattabile ai recapiti di Studio 0434/27969 o dpo@avvocatocorsini.it.	
TRATTAMENTO	*"*Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione*".* Qualunque tipo di operazione sui dati, con e senza l'ausilio di strumenti elettronici, costituisce trattamento.	
INFORMATIVA	Il titolare, anche attraverso i propri incaricati, deve fornire preventivamente all'interessato le informazioni di cui all'art. 13 del Regolamento circa la natura e le modalità del trattamento posto in essere, utilizzando i modelli predisposti dal titolare.	

CONSENSO DELL'INTERESSATO	Il consenso è la manifestazione di volontà che l'interessato dà circa l'utilizzo dei propri dati, pertanto ne costituisce necessario e preventivo presupposto l'informativa di cui all'art. 13. Se il trattamento riguarda dati sensibili o giudiziari, il consenso va espresso per iscritto. Sono previsti dalla Legge dei casi in cui è possibile effettuare il trattamento senza il consenso dell'interessato (ad es. per eseguire obblighi contrattuali o soddisfare richieste dell'interessato, anche in fase pre-contrattuale, come il caso dei fornitori; oppure per lo svolgimento di attività ritenute di pubblico interesse, come ad es. istruzione e formazione in ambito scolastico, professionale, superiore o universitario).
COMUNICAZIONE	"*Dare conoscenza dei dati personali a uno o più soggetti determinati ("destinatari") diversi dall'interessato, dagli incaricati o dal responsabile, in qualunque forma, anche mediante la loro messa a disposizione o consultazione*".
DIFFUSIONE	O divulgazione: "*Dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione*" (es. pubblicarli su internet).
NECESSITÁ	Uno dei principi fondamentali da rispettare è quello secondo cui non si devono trattare dati che non sono necessari al perseguimento delle finalità per cui sono utilizzati, perciò sono da evitare tutte le informazioni che non sono indispensabili alle mansioni lavorative. *Idem* i dati personali devono essere conservati per il tempo necessario, dopo di che, salvo obblighi di legge, essi vanno distrutti o cancellati.
LICEITÁ E CORRETTEZZA	I dati devono essere trattati in modo lecito e corretto, ovvero secondo la legge ed osservando il principio della buona fede contrattuale e precontrattuale. La violazione di predetti principi può comportare conseguenze giuridiche sul piano civile, penale ed amministrativo.

1.1.1 Introduzione

Questo documento fornisce agli incaricati del trattamento una panoramica sulle responsabilità loro spettanti rispetto alla gestione ed allo sviluppo della sicurezza dell'informazione.

Nell'ambito informatico, il termine "sicurezza" si riferisce a tre aspetti distinti:

Riservatezza: Prevenzione contro l'accesso non autorizzato alle informazioni;

Integrità: Le informazioni non devono essere alterabili da violazioni, incidenti o abusi;

Disponibilità: Il sistema deve essere protetto da interruzioni impreviste. Il titolare deve garantire la disponibilità dei dati, anche ai fini della continuità operativa nell'ambito di un pubblico servizio o di pubblico interesse.

Il raggiungimento di questi obiettivi richiede non solo l'utilizzo di appropriati strumenti tecnologici, ma anche gli opportuni meccanismi organizzativi; misure soltanto tecniche, per quanto possano essere sofisticate, non saranno efficienti se non usate propriamente.

In particolare, le precauzioni di tipo tecnico possono proteggere le informazioni durante il loro transito attraverso i sistemi, o anche quando queste rimangono inutilizzate su un disco di un computer; nel momento in cui esse raggiungono l'utente finale, la loro protezione dipende esclusivamente da quest'ultimo, e nessuno strumento tecnologico può sostituirsi al suo senso di responsabilità e al rispetto delle norme.

1. Linee guida per la sicurezza

UTILIZZATE LE CHIAVI

Il primo livello di protezione di qualunque sistema è quello fisico; è vero che una porta chiusa può 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 a chiave l'ufficio alla fine della giornata e chiudete i documenti a chiave nei cassetti o negli armadi ogni volta che potete.

CANCELLATE I DATI SE USATE COMPUTER CONDIVISI

Coloro i quali (ad es. gli insegnanti e gli allievi) che utilizzano i computer dei laboratori informatici 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. E' bene non salvare i dati personali (ad es. password) nei computer condivisi.

CONSERVATE I SUPPORTI DI MEMORIZZAZIONE IN UN LUOGO SICURO

Per i dischetti, o supporti di memorizzazione analoghi (es. le chiavette USB, hard disk esterni), si applicano gli stessi criteri che per i documenti cartacei, con l'ulteriore pericolo che il loro smarrimento (che può anche essere dovuto a un furto) può passare più facilmente inosservato. A meno che non siate sicuri che contengano solo informazioni non sensibili, riponeteli sotto chiave non appena avete finito di usarli. Prima di smaltirli tra i rifiuti, anche se apparentemente non funzionanti, è opportuno distruggerli.

UTILIZZATE LE PASSWORD

Vi sono svariate categorie di password, ognuna con il proprio ruolo preciso:

a) La password di accesso al computer impedisce l'utilizzo improprio della vostra postazione, quando per un motivo o per l'altro non vi trovate in ufficio.

b) La password di accesso alla rete impedisce che l'eventuale accesso non autorizzato a una postazione renda disponibili tutte le risorse dell'Ufficio.

c) La password dei programmi specifici permette di restringere l'accesso ai dati al solo personale autorizzato.

d) La password del salvaschermo, infine, impedisce che una vostra assenza momentanea permetta a una persona non autorizzata di visualizzare il vostro lavoro.

Imparate a utilizzare questi quattro tipi fondamentali di password, e mantenete distinta almeno quella di tipo *a),* che può dover essere resa nota, almeno temporaneamente, ai tecnici incaricati dell'assistenza. Scegliete le password secondo le indicazioni della sezione successiva.

Il sistema informatico dell'Ente è dotato di un "dominio" in cui sono definite le vostre credenziali personali: utilizzate sempre questo tipo di credenziali per l'accesso ai sistemi (PC, rete) per le vostre finalità lavorative.

ATTENZIONE ALLE STAMPE DI DOCUMENTI RISERVATI

Non lasciate accedere alle stampe persone non autorizzate; se la stampante non si trova sulla vostra scrivania recatevi quanto prima a ritirare le stampe. Distruggete personalmente le stampe quando non servono più, magari utilizzando un distruggi-documenti. Non lasciate incustodito il fax quando è in una zona accessibile a terzi.

NON LASCIATE TRACCIA DEI DATI RISERVATI

Quando rimuovete un file, i dati non vengono effettivamente cancellati ma soltanto marcati come non utilizzati, e sono facilmente recuperabili. Neanche la formattazione assicura l'eliminazione dei dati; solo l'utilizzo di un programma apposito garantisce che nel supporto utilizzato non resti traccia dei dati precedenti. Nel dubbio, è sempre meglio usare un supporto nuovo.

PRESTATE ATTENZIONE ALL'UTILIZZO DEI PC PORTATILI

I PC portatili sono un facile bersaglio per i ladri. Se avete necessità di gestire dati riservati su un portatile, fatevi installare un buon programma di cifratura del disco rigido, e utilizzate una procedura di backup periodico.

NON FATEVI SPIARE QUANDO STATE DIGITANDO LE PASSWORD

Anche se molti programmi non ripetono in chiaro la password sullo schermo, quando digitate la vostra password, questa potrebbe essere letta guardando i tasti che state battendo, anche se avete buone capacità di dattiloscrittura.

CUSTODITE LE PASSWORD IN UN LUOGO SICURO

Non scrivete la vostra password, meno che mai vicino alla vostra postazione di lavoro. L'unico affidabile dispositivo di registrazione è la vostra memoria. Se avete necessità di conservare traccia scritta delle password non lasciate in giro i fogli utilizzati, oppure consegnatene una copia in busta chiusa al Titolare.

NON FATE USARE IL VOSTRO COMPUTER A PERSONALE ESTERNO A MENO DI NON ESSERE SICURI DELLA LORO IDENTITÁ

Personale esterno può avere bisogno di installare del nuovo software/hardware nel vostro computer. Assicuratevi dell'identità della persona e delle autorizzazioni ad operare sul vostro PC.

NON INSTALLATE PROGRAMMI NON AUTORIZZATI

Solo i programmi con regolare licenza sono autorizzati. Se il vostro lavoro richiede l'utilizzo di programmi specifici, consultate il titolare ed il tecnico informatico individuato dall'Ente.

LIMITATE L'UTILIZZO DI SUPPORTI REMOVIBILI

L'utilizzo incontrollato dei supporti removibili può comportare dei rischi per la sicurezza delle informazioni: da un lato questi possono essere un punto di ingresso per minacce informatiche, come file dannosi per il sistema informatico dell'Ente, dall'altro se utilizzati per memorizzare informazioni riservate possono metterne a rischio la riservatezza, o perché possono essere più facilmente smarriti e finire nelle mani di persone non autorizzate, o se non correttamente gestiti (ad esempio cancellazione sicura dei dati).

Per tale ragione il loro uso va limitato e riservato alle necessità dell'Ente, adottando tutte le opportune cautele.

APPLICATE CON CURA LE LINEE GUIDA PER LA PREVENZIONE DA INFEZIONI DI VIRUS

La prevenzione dalle infezioni da virus sul vostro computer è molto più facile e comporta uno spreco di tempo molto minore della correzione degli effetti di un virus; tra l'altro, potreste incorrere in una perdita irreparabile di dati.

CONTROLLATE LA POLITICA LOCALE RELATIVA AI BACKUP

I vostri dati potrebbero essere gestiti da un *file server*, oppure essere gestiti in locale e trasferiti in un server solo al momento del backup. Verificate con il titolare la situazione e fate in modo che sia effettuato un salvataggio dei dati ad intervalli regolari. Non salvate i documenti e/o i file di lavoro solo all'interno del Vostro computer, ma salvateli all'interno di cartelle nel server affinchè siano oggetto di salvataggio e non ci sia rischio di perderli.

AVVISATE IL TITOLARE SE RITENETE CHE I DATI SIANO STATI VIOLATI

Allertate immediatamente il Titolare e il Responsabile della protezione dei dati 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.). Consultate la policy interna sul *data breach*.

2. Linee guida per la prevenzione dei virus

Un virus è un programma in grado di trasmettersi autonomamente e che può causare effetti dannosi.

Alcuni virus si limitano a riprodursi senza ulteriori effetti, altri si limitano alla semplice visualizzazione di messaggi sul video, altri ancora non danno segnali ma si "impadroniscono" dello strumento infettato, i più dannosi arrivano a distruggere o criptare tutto il contenuto del disco rigido.

COME SI TRASMETTE UN VIRUS:

1. Attraverso programmi provenienti da fonti non ufficiali.
2. Attraverso le macro dei programmi (ad es. un documento di word *.doc*).
3. Attraverso allegati o link contenuti nelle e-mail.

QUANDO IL RISCHIO DA VIRUS SI FA SERIO:

1. Quando si installano programmi di provenienza dubbia.
2. Quando si copiano dati da supporti non autorizzati.
3. Quando si scaricano dati o programmi da siti Internet sconosciuti o non attendibili.
4. Quando si aprono gli allegati alle email senza prestare la dovuta attenzione (vedi *infra*).
5. Quando si attivano i link indicati nelle email.

QUALI EFFETTI HA UN VIRUS?

1. Effetti sonori e messaggi sconosciuti appaiono sul video.
2. Nei menù appaiono funzioni extra finora non disponibili.
3. Le prestazioni del computer si rallentano inspiegabilmente.
4. Lo spazio disco residuo si riduce inspiegabilmente.
5. I file hanno un formato e un'estensione diversi dal solito e non si riescono ad aprire.
6. La navigazione web viene automaticamente inoltrata verso siti non richiesti.

COME PREVENIRE I VIRUS:

1. Usate soltanto programmi provenienti da fonti fidate.

   Copie sospette di programmi possono contenere virus o altro software dannoso. Ogni programma deve essere sottoposto alla scansione prima di essere installato. Non utilizzate programmi non autorizzati, con particolare riferimento ai videogiochi, che sono spesso utilizzati per veicolare virus.
2. Assicuratevi che il vostro software antivirus sia aggiornato, anche utilizzando la procedura manuale di aggiornamento dal menù dei programmi.
3. Non aprite allegati o cliccare i link presenti all'interno di email sospette e o di dubbia provenienza (vedi avanti per rischio da ransomware).
4. Limitate l'utilizzo dei supporti removibili a quelli strettamente necessari alle attività di pertinenza dell'Ente.

Scelta delle password

Il metodo più semplice per l'accesso illecito a un sistema consiste nell'indovinare la password dell'utente legittimo. In molti casi sono stati procurati seri danni al sistema informativo a causa di un accesso protetto da password "deboli". La scelta di password "forti" è, quindi, parte essenziale della sicurezza informatica.

COSA FARE

1. Usare password lunghe almeno otto caratteri (o, se inferiore, pari al massimo consentito) con un misto di lettere, numeri o segni di interpunzione. La password non deve contenere riferimenti agevolmente riconducibili all'incaricato (es. nome, cognome e anno di nascita *mariorossi72*), per cui NON usate il Vostro nome utente; è la password più semplice da indovinare.

2. NON usate password che possano in qualche modo essere legate a Voi come, ad esempio, il Vostro nome, quello di Vostra moglie/marito, dei figli, date di nascita, numeri di telefono etc.
3. Cambiare la password a intervalli regolari. Questa va modificata almeno ogni sei mesi o se il trattamento investe dati sensibili e/o giudiziari, ogni tre mesi.
4. NON dite a nessuno la Vostra password. Ricordate che lo scopo principale per cui usate una password è assicurare che nessun altro possa utilizzare le Vostre risorse o possa farlo a Vostro nome. Un eventuale illecito commesso da altri con le vostre credenziali potrebbe essere addebitato a voi
5. NON scrivete la password da nessuna parte che possa essere letta facilmente, soprattutto vicino al computer. Se ritenete di poter dimenticare la vostra password, conservatela in busta chiusa e consegnatela al titolare o a chi da questi incaricato.
6. Quando immettete la password NON fate sbirciare a nessuno quello che state battendo sulla tastiera.
7. Utilizzate password diverse per contesti diversi.

REGOLE ULTERIORI PER IL TRATTAMENTO DEI DATI E L'UTILIZZO DEGLI STRUMENTI INFORMATICI

- 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.
- 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.
- E' fatto divieto di utilizzare, sui sistemi informatici dell'Ente, dispositivi esterni per finalità diverse dalle attività di interesse e pertinenza dell'Ente stesso.
- E' fatto divieto di collegare alla rete informatica dell'Ente qualsiasi dispositivo personale (PC, smartphone, tablet, stampanti, scanner, chiavette USB)
- 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. Peraltro, si ricorda all'utilizzatore che assumono rilevanza 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..
- 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.
- 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).
- 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.

- Riponete i documenti cartacei al loro posto, o in altro luogo idoneo, al termine dell'orario di lavoro.
- Chiudete a chiave armadi e cassetti ogni volta che potete, specialmente per le stanze e gli archivi prossimi alle zone di attesa di terzi o in caso di stanze condivise. Lo stesso vale per i computer accesi in prossimità di zone promiscue degli uffici.
- *Non lasciare documenti sulla scrivania*. Non lasciare documenti, lettere, appunti sopra la scrivania quando vi allontanate dalla postazione di lavoro.
- Non lasciare il computer acceso se ci si assenta per un periodo più o meno lungo; potrebbe restare a disposizione di terzi non autorizzati. Se possibile utilizzate il blocco automatico con screensaver e password di ripristino.
- Assicuratevi di distruggere i documenti cartacei o i supporti elettronici/informatici che contengono dati personali prima di gettarli nel cestino.
- Non comunicare a nessun soggetto non specificatamente autorizzato, o della cui identità non siete certi, i dati personali comuni, sensibili, giudiziari e/o altri dati, elementi, informazioni dei quali venite a conoscenza nell'esercizio delle vostre funzioni e mansioni. 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.
- Non portare via dall'ufficio documenti o copie di documenti (cartacei e/o elettronici) se non per il normale svolgimento delle mansioni di lavoro o se richiestovi dal titolare del trattamento.

POSTA ELETTRONICA (E-MAIL)

Corretto utilizzo degli indirizzi e-mail assegnati all'utente:

- Le caselle di posta elettronica aziendale date in uso all'utente (ad es. *dipendente@datoredilavoro.it o più semplicemente farmaciaxyz@libero.it*) sono destinate ad un utilizzo tassativamente ed esclusivamente inerente all'attività lavorativa e non devono essere utilizzate per scopi personali.
- Inoltre è fatto divieto di configurare all'interno del programma su pc di gestione della posta elettronica indirizzi personali non relativi ai domini di posta lavorativi, quali ad esempio quelli forniti gratuitamente dai provider (@libero.it, @yahoo.com, @gmail.com, ecc.).
- L'utente non deve utilizzare l'indirizzo di posta elettronica aziendale per iscriversi a newsletter, mailing list, forum, chat, ecc., salvo che questi servizi siano inerenti all'attività lavorativa (ad es. su siti web istituzionali di categoria); in caso di dubbio, l'utente deve rivolgersi al titolare del trattamento.
- E' vietato configurare l'email istituzionale su applicativi di gestione della posta elettronica installati 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.
- 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.
- La stessa accortezza nella verifica della corretta compilazione dei form di invio va prestata comunque in caso di invio di comunicazioni riservate o dal contenuto personale.
- L'utente deve utilizzare la posta elettronica in modo appropriato e consapevole:

  1. 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.
  2. 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.

3. 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.
4. 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.

Rapporti con gli utenti dell'Istituto

Quando si ricevono soggetti terzi (cittadini, rappresentanti, genitori, ecc.) sincerarsi che nessun documento contenente dati personali e/o sensibili o informazioni riservate possa risaltare alla vista degli stessi; ove possibile capovolgere le facciate dei documenti per tutta la durata del servizio; se necessario non abbandonare presso il fotocopiatore documenti leggibili, tenere il fax lontano dalla vista di chi non è incaricato.

[1] https://www.certnazionale.it/documenti/2016/05/05/ransomware-rischi-e-azioni-di-prevenzione/

Diritti degli interessati e diritto di accesso

Gli artt. 15 e seguenti del Regolamento UE 679/2016 prevedono che tutti i soggetti interessati (in particolare gli allievi e i dipendenti) possano esercitare nei confronti del titolare i diritti che la Legge riserva loro, e segnatamente:

Art. 15. *Diritto di accesso dell'interessato.*

Art. 16. *Diritto di rettifica.*

Art. 17. *Diritto alla cancellazione («diritto all'oblio»).*

Art. 18. *Diritto di limitazione di trattamento.*

Art. 20. *Diritto alla portabilità dei dati.*

Art. 21. *Diritto di opposizione.*

Art. 22. Diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione.

Dal momento che tali diritti possono essere fatti valere nei confronti del titolare del trattamento o del responsabile del trattamento, senza particolari formalità (quindi sia oralmente che per iscritto), anche attraverso i suoi incaricati, si raccomanda, nell'ipotesi appena illustrata, di avvertire immediatamente il titolare o il responsabile del trattamento.

Nel caso di istanza scritta, infatti, i tempi di riscontro sono relativamente brevi. Recita l'art. 12: "*Il titolare del trattamento fornisce all'interessato le informazioni relative all'azione intrapresa riguardo a una richiesta ai sensi degli articoli da 15 a 22 senza ingiustificato ritardo e, comunque, al più tardi* ***entro un mese dal ricevimento della richiesta*** *stessa. Tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste, previo avviso all'interessato*".

Nel caso di istanza presentata personalmente dall'interessato, così come in caso di ricezione tramite altri canali (avvocati o procuratori degli aventi diritto), **è obbligatorio sincerarsi preventivamente dell'identità del richiedente** con ogni modalità idonea (documento di identità e, per avvocati e procuratori/tutori, del mandato o del documento attestante la qualifica).

Per ogni altra informazione o delucidazione in merito al comportamento da tenersi o alle operazioni da effettuarsi è necessario rivolgersi al Titolare del trattamento o ai soggetti da egli specificamente designati.

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