POLICY
B.Y.O.D. | BRING YOUR OWN DEVICES

COD. C.16
VERS. 01 DEL 05.2022

CONTIENE:

1. **POLICY**

INDICE DELLE VERSIONI SUCCESSIVE ALLA PRIMA:

COD. VERSIONE	DATA MODIFICA	MODIFICHE

PREMESSA

La prassi volta all'utilizzo del proprio computer, anche per attività lavorativa, nasce diversi anni fa per rendere l'approccio alla macchina più confidente da parte del lavoratore. Tuttavia, con il periodo pandemico, si è passati a utilizzare il proprio computer per motivi di opportunità ad usarlo per esigenze pratiche. Le scuole non erano difatti in possesso di sufficienti device da consegnare a tutti i docenti per portare avanti le lezioni da distanza e, quindi, è stato necessario per il personale della scuola iniziare ad utilizzare i computer personali. Questo ha portato vantaggi e svantaggi, primo fra tutti il fatto di condividere uno strumento di lavoro con il resto della famiglia, aumentando così in modo sensibile il rischio di data breach e di accesso non autorizzato ai dati degli interessati.

PERICOLI PRINCIPALI

I pericoli principali da evitare sono i seguenti:

- Accesso di un familiare alle informazioni archiviate sul device
- Pubblicazione involontaria, da parte anche di familiari, di informazioni presenti sul device utilizzato dal personale scolastico per fini istituzionali
- Rischio di installazione di malware e di infezione di sistemi scolastici
- Copiatura e condivisione di informazioni riservate
- Modifica di informazioni degli interessati da parte, ad esempio, di un familiare
- Accesso, da parte di familiari, ai sistemi scolastici (es: registro elettronico) per motivi non riconducibili all'attività lavorativa

COME COMPORTARSI

Al fine di scongiurare la maggior parte dei predetti problemi è in primo luogo possibile dotarsi di un duplice account sul medesimo device: un account, con password, dedicato all'attività lavorativa e l'altro account dedicato all'attività domestica.
In questo modo, ad esempio, i parenti del docente non potranno in alcun modo accedere ai dati degli studenti, eliminando alla radice ogni criticità che potrebbe derivare dall'accesso o dalla diffusione di dati trattati dal personale scolasti per ragioni inerenti il proprio ruolo professionale.

MISURE DI SICUREZZA

Il Dirigente, prima di autorizzare l'utilizzo di sistemi domestici per fini lavorativi, deve necessariamente sottoporre i device in questione ad una analisi volta a comprendere il grado di sicurezza degli stessi. In particolare, l'esame deve volgere sui seguenti parametri:

1. Il Sistema Operativo deve essere recente e garantire la presenza di aggiornamenti
2. Il device deve essere dotato di sistemi di protezione quali antivirus e simili
3. Il device deve essere connesso e compatibile ai sistemi di repository e backup predisposti dalla scuola
4. Non salvare dati della scuola su device personali
5. Il personale deve essere necessariamente formato
6. La scuola deve regolamentare l'accesso alle reti LAN, internet e wi-fi inventariando i dispositivi sulla base di quanto disposto dalle linee guida Agid sulle misure minime ICT del 2017

IN SINTESI

In generale, al fine di utilizzare i propri device è necessario seguire le seguenti istruzioni in modo pedissequo:

1. Assicurarsi di accedere al sistema operativo con un account riservato all'attività lavorativa e dotato di password sicura
2. Utilizzare sistemi operativi per i quali è garantito il supporto ed effettuare costantemente gli aggiornamenti

3. Assicurarsi che i software antivirus siano abilitati e costantemente aggiornati
4. Non installare software provenienti da fonti non ufficiali
5. Non cliccare su link o allegati contenuti in email sospette
6. Utilizzare l'accesso a connessioni Wi-Fi protette
7. Collegarsi a dispositivi mobili (es. pen drive e hard disk esterni) previamente formattate e di cui si conosce la provenienza
8. Allestire la postazione di lavoro in modo da garantire la riservatezza dei dati ed effettuare il log-out dai servizi/portali utilizzati dopo che è stata conclusa la sessione lavorativa

CORRETTO UTILIZZO DI CHIAVETTE USB

In linea generale, è da ritenersi vietato l'utilizzo di chiavette USB a scuola dovendosi preferire l'invio di informazioni tramite e-mail, registro elettronico o altro strumento idoneo autorizzato dalla scuola e dal DPO.

Solo ed esclusivamente qualora ciò non sia possibile, dovendo necessariamente ricorrere alla pen drive, sarà da considerarsi autorizzato l'uso della stessa ma solo alle seguenti condizioni:

- La pen drive deve essere nuova o, comunque, formattata prima dell'uso, specie se si è in procinto di trasferire dati da un computer all'altro
- La pen drive, anche se utilizzata per trasferire dati, completato il passaggio deve necessariamente subire una formattazione con contestuale eliminazione di tutto il contenuto
- La pen drive non deve in nessun caso essere utilizzata come archivio di dati personali, nemmeno per breve tempo
- Il personale, in concomitanza con l'eventuale trasferimento di dati tramite pen drive, è tenuto a non perdere di vista tale chiavetta, mantenendone sempre il controllo, anche e soprattutto quando altro soggetto effettua operazioni di upload o download