ISTITUTO COMPRENSIVO
"C. SALUTATI - A. CAVALCANTI"
Piazza A. Moro, 1 – 51011 Borgo a Buggiano (PT)
C.F.: 81003470473 - tel. 0572 - 32018
ptic81900g@istruzione.it – ptic81900g@pec.istruzione.it www.istitutosalutaticavalcanti.it

Prescrizioni in caso di utilizzo di dispositivi personali (BYOD)

L'utilizzo di dispositivi personali (BYOD) è consentita solo previa autorizzazione del proprio responsabile.

Il dipendente accetta di rispettare le seguenti indicazioni generali finalizzate a garantire la protezione dei dati riservati memorizzati o a cui si accede utilizzando un dispositivo mobile personale utilizzato nell'ambito dell'attività lavorativa, anche ai sensi della presente procedura:

- fare quanto necessario per garantire l'adeguata sicurezza fisica del dispositivo e più specificamente custodire i dispositivi mobili personali con la diligenza necessaria sia durante gli spostamenti, sia durante l'utilizzo nel luogo di lavoro, adottando tutti gli accorgimenti che le circostanze rendono necessari per evitare danni o sottrazioni di dati, ad esempio non lasciando incustoditi i dispositivi portatili in auto, su treni o aerei. In particolare, i dispositivi devono sempre essere protetti da sistemi di autenticazione e da altre misure di sicurezza come antivirus e screensaver;
- rispettare il Regolamento per l'utilizzo della strumentazione informatica istituzionale e della rete internet per la tutela della privacy;
- garantire la cifratura dei dati confidenziali dell'Istituto nel caso in cui vengano memorizzato all'interno del dispositivo personale;
- aggiornare regolarmente il sistema operativo e le applicazioni del dispositivo;
- assicurare che i controlli di sicurezza del dispositivo mobile non vengano sovvertiti da hack, jailbreak, root, modifiche al software di sicurezza e/o alle impostazioni di sicurezza;
- effettuare il backup di tutti i dati, delle impostazioni, dei supporti e delle applicazioni;
- segnalare immediatamente un dispositivo mobile smarrito o rubato, come indicato nella procedura riportata in calce alle presenti istruzioni;
- comunicare prontamente al titolare del trattamento dati, il dirigente scolastico, ogni tipo di altra violazione dei dati che il dispositivo dovesse subire a causa di un evento di sicurezza;
- utilizzare sempre una rete Wi-Fi sicura protetta da adeguate chiavi di cifratura e credenziali di accesso;

I rischi principali in cui incorre l'Istituto nel caso dell'utilizzo di dispositivi personali (BYOD) da parte dei dipendenti possono essere così sintetizzati:

- *Local exposure*: si intende la perdita di controllo dei dati di titolarità dell'Istituto, che vengono trasmessi, archiviati ed elaborati sui dispositivi personali dei dipendenti;
- perdita di dati: il BYOD può portare alla potenziale perdita o divulgazione dei dati personali da un dispositivo non protetto oppure causata dal furto del dispositivo;
- esposizione pubblica dei dati: usare dispositivi personali nel luogo di valoro aumenta il rischio di attacchi e intercettazione dei dati, soprattutto quando il dipendente si connette via hotspot, Wi-Fi pubblico o tramite Bluetooth;
- app dannose: un dipendente potrebbe avere la teorica possibilità di installare app potenzialmente dannose: un esempio sono le notifiche push o l'abilitazione dei servizi di geolocalizzazione, che possono compromettere le applicazioni attendibili sul dispositivo;
- personalizzazione delle impostazioni di sicurezza: gli utenti di dispositivi ad uso personale solitamente rimuovono le restrizioni imposte dai fornitori, ma così facendo

rendono il dispositivo più vulnerabile alle applicazioni non sicure, che accedono ai dati di titolarità dell'Istituto;

- attacchi interni: si tratta di vulnerabilità difficili da rilevare dato che si verificano nella rete LAN locale da qualcuno che vi accede con un profilo utente valido.

In considerazione dei rischi sopra evidenziati, si raccomanda pertanto di attenersi con il massimo scrupolo alle regole di comportamento indicate nel presente paragrafo nell'utilizzo di BYOD allo scopo di ridurre i rischi consentire un utilizzo sicuro dei BYOD.

Procedura da seguire in caso di smarrimento o furto di dispositivi informatici

In caso di furto o smarrimento di dispositivi informatici l'Utente dovrà attenersi alla seguente procedura:

a. modificare tutte le password di dominio e di accesso ad eventuali applicativi installati sul dispositivo rubato immediatamente appena scoperto il furto;
b. segnalare al titolare del trattamento dati, il dirigente scolastico l'avvenuto smarrimento o furto, attraverso la seguente e-mail ptic81900g@istruzione.it entro e non oltre 8 ore dall'avvenuto furto/smarrimento;
c. indicare, per iscritto, in modo dettagliato, i dati contenuti nel dispositivo smarrito o rubato;
d. rimanere a disposizione per ulteriori richieste di informazioni, rendendosi reperibile nelle immediatezze della segnalazione.