Sommario

1. PREMESSA 2
2. OBBLIGHI DEL LAVORATORE IN MODALITÀ SMART WORKING 2
3. LE BUONE PRASSI PER LAVORARE DA CASA IN SICUREZZA 2
4. REGOLE DA OSSERVARE PER L'UTILIZZO DI DISPOSITIVI PERSONALI – BYOD POLICY 3
5. LE CONNESSIONI DOMESTICHE 3
6. ATTENZIONE AL PISHING 3

1. Premessa

Con il presente documento sono individuate le linee di condotta e le procedure da rispettare in tutti i casi in cui i Dipendenti e/o i Collaboratori svolgano, anche occasionalmente o in via eccezionale, previa autorizzazione o, comunque, nell'ambito delle proprie mansioni formalmente individuate, attività lavorative in luoghi diversi da quelli dell'Istituto. La modalità di lavoro in smart working prevede il rispetto di alcune norme per lavorare in sicurezza e proteggere i dati personali e le informazioni inerenti l'Istituto anche fuori dai luoghi istituzionali.

2. Obblighi del lavoratore in modalità Smart Working

Ogni dipendente o collaboratore dovrà attenersi alle seguenti indicazioni di carattere generale:

a) Ottemperare alle regole di riservatezza e/o alle procedure già previste dall'Istituto (es. il Regolamento sul corretto utilizzo dei dispositivi).
b) Adottare ogni mezzo ragionevole per proteggere le informazioni acquisite al fine di prevenire la divulgazione delle stesse.
c) Garantire la massima diligenza nell'uso della strumentazione assegnata ai fini dell'esecuzione dell'attività lavorativa, nonché la sicurezza, anche fisica, dei dati contenuti nei dispositivi concessigli in uso dal Datore di lavoro.
d) Non comunicare e/o diffondere a terzi dati ed informazioni trattati e/o comunque appresi in ragione dell'esecuzione del rapporto di lavoro, anche nel caso di familiari.
e) Nel caso in cui l'attività lavorativa sia svolta all'interno della propria abitazione, il dipendente/collaboratore si impegna ad adottare tutte le misure tecnico-organizzative più opportune al fine di evitare che detti dati ed informazioni riservati vengano a conoscenza di terzi non autorizzati.

3. Le buone prassi per lavorare da casa in sicurezza

a) Svolgere l'attività se possibile in un locale in cui sia impedito l'accesso a terzi (anche familiari) durante l'attività lavorativa. In caso contrario, non lasciare mai incustoditi i dispositivi utilizzati per la prestazione lavorativa.
b) Ridurre al minimo il materiale cartaceo, nel caso la gestione di dati su supporto cartaceo fosse indispensabile, al termine dell'attività lavorativa lo stesso dovrà essere riposto impedendone l'accesso a terzi (es. in cassetti chiusi a chiave).
c) Connettersi alla rete dell'Istituto solo tramite reti sicure (ad esempio tramite VPN se sono state messe a disposizione dal datore di lavoro).
d) Utilizzare gli strumenti di condivisione messi a disposizione dall'Istituto o da esso autorizzati (es. Sharepoint, Google Drive, posta elettronica) evitando applicazioni con utenze private (es. utenza Drop Box privata, WhatsApp).
e) Utilizzare unicamente i software e le applicazioni autorizzate e fornite dall'Istituto;
f) Effettuare con regolarità gli aggiornamenti del sistema operativo e dell'antivirus presenti sul dispositivo utilizzato.
g) Evitare di salvare i documenti sullo schermo del pc (policy di "clear screen"),
h) Non lasciare incustodito il dispositivo in dotazione, che dovrà essere spento o messo in stand by alla fine di ogni sessione di lavoro, anche con lo screen saver protetto da password dopo 10 minuti di inattività.
i) Evitare lo svolgimento dell'attività di lavoro presso locali pubblici o aperti al pubblico, salvo specifiche esigenze lavorative.

4. Regole da osservare per l'utilizzo di dispositivi personali – BYOD policy

Se non si è dotati di un dispositivo di proprietà dell'Istituto o non è stato possibile portare con se quelli in dotazione (a seguito di situazioni contingenti o di emergenza), per consentire l'operatività dell'Istituto è permesso l'utilizzo dei dispositivi privati. Si riporta di seguito la policy BYOD ("Bring Your Own Device" – Porta con se il tuo dispositivo) con le indicazioni di utilizzo in sicurezza.

a) aggiornare regolarmente il sistema operativo e le applicazioni installate sui dispositivi;
b) evitare la memorizzazione di dati dell'Istituto su app non approvate;
c) evitare di effettuare modifiche alle configurazioni software dei dispositivi, perché questi potrebbero eludere i controlli di sicurezza;
d) effettuare con regolarità il back up dei dati presenti sul dispositivo;
e) eventuali dispositivi smarriti o violazioni di dati devono essere immediatamente comunicati alla Direzione scolastica;
f) custodire i dispositivi mobili con diligenza in caso di spostamenti e non consentirne l'utilizzo promiscuo, in alternativa creare utenze diverse da quelle utilizzate per il lavoro;
g) mantenere pin e password su tutti i dispositivi.

<u>Utilizzo degli smart assistant</u>

Durante il lavoro da casa possono essere scambiate informazioni riservate via telefono o videoconferenza.
In presenza di smart assistant all'interno delle abitazioni (es. Alexa, Google Home, ecc.):

a) disattivare l'assistente digitale quando non viene utilizzato;
b) non utilizzare gli smart assistant per effettuare operazioni di lavoro.

5. Le connessioni domestiche

a) Non è consentito l'utilizzo di reti pubbliche per lo svolgimento dell'attività lavorativa.
b) Nel caso non fosse fornita una connessione dall'Istituto, al fine di garantire una maggiore sicurezza delle connessioni domestiche si raccomanda di cambiare le password dei default della connessione ADSL/Wi-fi o del router qualora queste non fossero sufficientemente complesse (es. 123456, Admin, 0000, ecc.).
c) È consigliabile scegliere una password contenente almeno 15 caratteri alfanumerici senza frasi di senso compiuto o relative all'Istituto, al nome del prodotto o all'utente.

6. Attenzione al pishing

La comunicazione lavorativa in modalità smartworking può essere molto diversa da quella ordinaria, specie in situazioni contingenti o di emergenza. Alcune richieste possono essere ricevute con qualche deroga alle procedure abitualmente adottate. Le regole da seguire per garantire la sicurezza dei dati e delle informazioni:

a) Controllare sempre l'attendibilità delle mail: lay-out del messaggio, firma, ora dell'invio.
b) Non aprire mai allegati eseguibili, ovvero file che hanno come estensione ".exe".
c) Nel dubbio chiedere al mittente se ha davvero inviato il messaggio.
d) In caso di richieste di pagamento o di dati riservati confermare sempre con il mittente via telefono per verificare che siano reali e autorizzate.