ISTITUTO PROFESSIONALE DI STATO
PER I SERVIZI ALBERGHIERI E DELLA RISTORAZIONE
" PELLEGRINO ARTUSI "
(Cod. RARH020004)

Distr.scol.n. 41 Via Tarlombani, 7 - 48025 Riolo Terme (RA) - Cod.Fisc. 90003100394
www.alberghieroriolo.edu.it Tel.: 054671113 - 054671636 - 054671851 Fax: 054671859 Codice univoco fatt. elettr. UFBLHI
E-mail: rarh020004@istruzione.it E-mail cert. (PEC): rarh020004@pec.istruzione.it

REGOLAMENTO BYOD - *BRING YOUR OWN DEVICES*

Regolamento per l'utilizzo dei dispositivi digitali personali

II. UTILIZZO DI DISPOSITIVI PERSONALI IN REGIME DI "LAVORO AGILE" – P.ATA

Al fine di garantire la sicurezza del trattamento dei dati personali anche con riferimento alle categorie particolari (ex dati sensibili), l'Istituto Alberghiero di Riolo Terme (RA) disciplina le modalità di svolgimento del Lavoro Agile estendendo le prescrizioni e le procedure organizzative previste sul luogo di lavoro anche nell'adempimento di attività e mansioni da remoto.

Norme di comportamento per gli assistenti amministrativi al trattamento dei dati

L'incaricato del trattamento è tenuto a prediligere il Lavoro Agile su un terminale fornito direttamente dall'Istituto scolastico, in quanto opportunamente configurato per gestire dati personali in piena sicurezza. Qualora l'istituto non dovesse garantire la consegna di terminali inventariati, si raccomanda l'incaricato di utilizzare il dispositivo personale rispettando le seguenti istruzioni:

1. Assicurarsi di non effettuare forme di salvataggio dati di pertinenza dell'istituto sui propri device;
2. Gestire il proprio lavoro mediante accesso a piattaforme (es. segreteria digitale) e soluzioni di Cloud attivate, evitando l'uso di altre soluzioni di terze parti non espressamente autorizzate dall'Istituto;
3. Limitare l'utilizzo del dispositivo al solo incaricato, evitando durante le attività lavorative la condivisione del terminale con altri soggetti non espressamente autorizzati;
4. Prediligere la navigazione in incognito, al fine di garantire riservatezza qualora il dispositivo fosse soggetto ad uso promiscuo;
5. Su richiesta dell'Istituto è possibile installare software per il "Desktop Remote control" ovvero effettuare accesso ad una VPN;
6. Mantenere attiva l'opzione di aggiornamento automatico del S.O. in uso (Windows, Linux, macOS);
7. Utilizzare sempre e solo indirizzi email con dominio istituzionale, evitando email personali non autorizzate;
8. Predisporre la cifratura dei file (inserimento password) quando la stessa si rende necessaria in ragione della natura dei dati trattati (es. documenti contenenti informazioni particolari

dell'utenza come stati di salute ecc…);

9. custodire con la massima diligenza le credenziali di autenticazione (user-id e password) per l'utilizzo del computer e per l'accesso alle banche dati e ai sistemi informativi di competenza;

12. mantenere riservata la propria password evitando qualsiasi forma di condivisione;

13. modificare la password almeno ogni sei mesi. Nel caso in cui la password dia l'accesso a dati personali particolari o giudiziari, essa deve essere modificata almeno ogni tre mesi. La password deve essere composta da almeno 8 caratteri (nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito) e non deve contenere riferimenti facilmente riconducibili all'incaricato;

14. presenziare, quando possibile, agli interventi di assistenza e digitare personalmente la propria password. Qualora ciò non sia possibile, provvedere alla modifica alla password immediatamente dopo l'intervento;

15. non collegare modem o dispositivi che consentano un accesso non controllato al computer e alla rete d'Istituto

16. non utilizzare supporti removibili (CD, DVD, PenDrive) di provenienza esterna e, qualora ciò si rivelasse necessario, verificare sempre preliminarmente l'integrità dei supporti con il programma antivirus installato;

17. non scaricare file eseguibili o documenti di testo da siti internet senza verificare l'assenza di virus;

18. non disabilitare la password di screen saver, per evitare accessi non autorizzati quando la postazione non é presidiata;

19. non condividere il proprio hard disk con un altro computer se non in condizioni di protezione da scrittura e con password di accesso;

20. non riutilizzare supporti removibili sui quali siano conservati dati sensibili o giudiziari a meno che i dati in essi contenuti non siano intelleggibili e tecnicamente ricostruibili. Diversamente, i supporti removibili debbono essere distrutti;

DIRIGENTE SCOLASTICO

Prof. Stefano Rotondi

(firmato digitalmente ai sensi del CAD e delle norme ad esso connesse)