POLICY
GESTIONE DELLE SCRIVANIE E SCHERMI PULITI

COD. C.19
VERS. 01 DEL 05.2022

CONTIENE:

1. **POLICY**

INDICE DELLE VERSIONI SUCCESSIVE ALLA PRIMA:

COD. VERSIONE	DATA MODIFICA	MODIFICHE

PREMESSA

Per migliorare la sicurezza e la riservatezza delle informazioni, la presente istituzione scolastica adotta una politica finalizzata a garantire la presenza di una scrivania e di un desktop sempre in ordine. Questo al fine di ridurre il rischio di accessi non autorizzati, perdita e danneggiamento di informazioni durante e al di fuori del normale orario di lavoro o quando le aree non sono presidiate.

MODALITÀ OPERATIVE

Quanto alla scrivania pulita si richiede di rispettare le seguenti indicazioni:

1. Carta e supporti di archiviazione esterna (ove autorizzati) devono essere custoditi in appositi archivi fisici chiusi a chiave in stanze non accessibili al pubblico
2. I visitatori della scuola, ma anche i familiari e gli studenti, non devono in alcun modo avere accesso ai locali ove sono presenti i device utilizzati dal personale scolastico e agli archivi cartacei
3. Informazioni riservate, sensibili o classificate, una volta stampate, devono essere rimosse immediatamente dalle stampanti. Ove possibile, devono essere utilizzate le stampanti con l'opzione di inserimento password per la protezione dei documenti
4. Prima di gettare i documenti è necessario distruggerli in modo tale da non renderli facilmente ricomponibili
5. Notare che le informazioni lasciate sulla scrivania hanno più probabilità di essere danneggiate o distrutte in una situazione di emergenza come incendio, inondazione o esplosione
6. Non stampare le email per leggerle: è una scelta non ecologica ed aumenta il pericolo di disordine
7. Liberare sempre la scrivania prima di andare a casa

Quanto invece alla pulizia del desktop, si chiede al personale di attenersi scrupolosamente alle seguenti indicazioni:

1. Gli utenti devono SEMPRE effettuare "log-off" (disconnettersi) dai principali servizi utilizzati quanto gli stessi sono stati oggetto di sessione su un device condiviso
2. Gli utenti devono attivare salva schermi automatici in modo da impedire l'accesso alle informazioni in caso di device lasciato incustodito per brevi istanti (es: per fruire dei servizi igienici)
3. Il salva schermo deve essere protetto da password per la riattivazione
4. Le password non devono essere annotate nelle vicinanze del device utilizzando, ad esempio, fogliettini adesivi e simili