



ISTITUTO PROFESSIONALE DI STATO
PER I SERVIZI COMMERCIALI, TURISTICI E SOCIALI
“PAOLO BOSELLI”

**LINEE GUIDA IN MATERIA DI SICUREZZA
PER IL COLL. SCOLASTICO INCARICATO DEL TRATTAMENTO**

Vengono di seguito indicate le misure operative da adottare per garantire la sicurezza dei dati personali indicate nel Documento Programmatico sulla Sicurezza:

- Accertarsi che al termine delle lezioni non restino incustoditi i seguenti documenti, segnalandone tempestivamente l'eventuale presenza al responsabile di sede e provvedendo temporaneamente alla loro custodia:
 - a. Registro personale dei docenti
 - b. Registro di classe
 - c. Certificati medici esibiti dagli alunni a giustificazione delle assenze
 - d. Qualunque altro documento contenente dati personali o sensibili degli alunni o dei docenti
- Accertarsi che al termine delle lezioni tutti i computer dell'aula di informatica siano spenti e che non siano stati lasciati incustoditi floppy disk, cartelle o altri materiali, in caso contrario segnalarne tempestivamente la presenza al responsabile di laboratorio o di sede e provvedendo temporaneamente alla loro custodia.
- Verificare la corretta funzionalità dei meccanismi di chiusura di armadi che custodiscono dati personali, segnalando tempestivamente al responsabile di sede eventuali anomalie.
- Procedere alla chiusura dell'edificio scolastico accertandosi che tutte le misure di protezione dei locali siano state attivate.
- Effettuare esclusivamente copie fotostatiche di documenti per i quali si è autorizzati.
- Non lasciare a disposizione di estranei fotocopie inutilizzate o incomplete di documenti che contengono dati personali o sensibili ma accertarsi che vengano sempre distrutte.
- Non lasciare incustodito il registro contenente gli indirizzi e i recapiti telefonici del personale e non annotarne il contenuto sui fogli di lavoro.
- Non abbandonare la postazione di lavoro per la pausa o altro motivo senza aver provveduto a custodire in luogo sicuro i documenti trattati
- Non consentire che estranei possano accedere ai documenti dell'ufficio o leggere documenti contenenti dati personali o sensibili.
- Segnalare tempestivamente al Responsabile del trattamento la presenza di documenti incustoditi e provvedere temporaneamente alla loro custodia.
- Procedere alla chiusura dei locali non utilizzati in caso di assenza del personale.
- Procedere alla chiusura dei locali di segreteria accertandosi che siano state attivate tutte le misure di protezione e che le chiavi delle stanze siano depositate negli appositi contenitori.
- Attenersi alle direttive ricevute e non effettuare operazioni per le quali non si è stati espressamente autorizzati dal Responsabile o dal Titolare.

Riguardo ai trattamenti eseguiti con supporto informatico attenersi scrupolosamente alle seguenti indicazioni:

- Non lasciare floppy disk, cartelle o altri documenti a disposizione di estranei;
- Conservare i dati sensibili in armadi chiusi, ad accesso controllato o in files protetti da password;
- Non consentire l'accesso ai dati a soggetti non autorizzati;
- Riporre i supporti in modo ordinato negli appositi contenitori e chiudere a chiave classificatori e armadi dove sono custoditi;
- Scegliere una password con le seguenti caratteristiche:
 - Originale
 - Composta da almeno sei caratteri
 - Evitando il nome proprio, il nome di congiunti, date di nascita e comunque riferimenti alla propria persona o lavoro facilmente ricostruibili
- Curare la conservazione della propria password ed evitare di comunicarla ad altri;
- Cambiare periodicamente (almeno una volta ogni tre mesi) la propria password;
- Modificare prontamente (ove possibile) la password assegnata;
- Spegnerne correttamente il computer al termine di ogni sessione di lavoro;
- Non abbandonare la propria postazione di lavoro senza essersi disconnessi dal proprio profilo personale o aver inserito uno screen saver con password;
- Comunicare tempestivamente al Titolare o al Responsabile qualunque anomalia riscontrata nel funzionamento del proprio profilo di accesso alla rete;
- Non riutilizzare i supporti informatici utilizzati per il trattamento di dati sensibili per altri trattamenti;
- Non gestire informazioni su più archivi ove non sia strettamente necessario e comunque curarne l'aggiornamento in modo organico;
- Utilizzare le seguenti regole per la posta elettronica:
 - a. Non aprire documenti di cui non sia certa la provenienza
 - b. Non aprire direttamente gli allegati ma salvarli su disco e controllarne il contenuto con un antivirus
 - c. Controllare accuratamente gli indirizzi dei destinatari prima di inviare dati personali

IL DIRIGENTE SCOLASTICO
Titolare del trattamento dati