

LINEE GUIDA IN MATERIA DI SICUREZZA PER IL COLLABORATORE SCOLASTICO INCARICATO DEL TRATTAMENTO

Vengono di seguito indicate le misure operative da adottare per garantire la sicurezza dei dati personali:

Per i Collaboratori Scolastici in servizio nelle sedi ed ai piani

- Accertarsi che al termine delle lezioni non restino incustoditi i seguenti documenti, segnalandone tempestivamente l'eventuale presenza al Responsabile di plesso e provvedendo temporaneamente alla loro custodia:
 - Registro personale dei docenti
 - Registro di classe
 - certificati medici esibiti dagli alunni a giustificazione delle assenze
 - qualunque altro documento contenente dati personali o sensibili degli alunni o dei docenti.
- Accertarsi che al termine delle lezioni tutti i computer delle aule siano spenti e che non siano stati lasciati incustoditi supporti di memoria informatici (chiavette USB, DVD, ecc.), cartelle o altri materiali, in caso contrario segnalarne tempestivamente la presenza al Responsabile di plesso provvedendo temporaneamente alla loro custodia.
- Verificare la corretta funzionalità dei meccanismi di chiusura degli armadi che custodiscono dati personali, segnalando tempestivamente al Responsabile di plesso eventuali anomalie.
- Procedere a chiudere a chiave al termine della giornata la stanza individuata come sala docenti
- Procedere alla chiusura dell'edificio scolastico accertandosi che tutte le misure di protezione dei locali siano state attivate.

Per i Collaboratori Scolastici a supporto della Segreteria o della produzione della documentazione

- 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 Titolare 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 stati espressamente autorizzati dal Titolare.

Uso di PC e dell'account d'Istituto:

- non memorizzare file contenenti dati personali e/o sensibili nei PC
- non lasciare supporti di memoria informatici (chiavette USB, DVD, ecc.), cartelle o altri documenti contenenti dati personali e/o sensibili a disposizione di estranei
- non consentire nel modo più assoluto agli alunni l'accesso alla LIM e ai PC dei laboratori, se non in presenza dei docenti
- per l'uso e della Posta elettronica/Account d'Istituto, scegliere una password con le seguenti caratteristiche:
 - originale
 - composta da almeno otto caratteri
 - che contenga almeno un numero una lettera e un carattere speciale
- che non sia facilmente intuibile, 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 la password assegnata

- spegnere correttamente il computer al termine di ogni sessione di lavoro o, nel caso in cui debba essere utilizzato da altro utente, mettere in atto le apposite misure di sicurezza
- uscire dall'account prima di lasciare la postazione di lavoro promiscua, si consiglia di utilizzare il browser in modalità "navigazione anonima"
- comunicare tempestivamente qualunque anomalia riscontrata nel funzionamento del computer
- utilizzare le seguenti regole per la Posta elettronica e la condivisione dei documenti:
 - non aprire documenti di cui non sia certa la provenienza
 - non aprire direttamente gli allegati ma salvarli su disco e controllarne il contenuto con un antivirus
 - controllare accuratamente l'indirizzo dei destinatario o l'account qualora sia necessario inviare/condividere documenti contenenti dati personali

Qualunque violazione delle modalità sopra indicate dà luogo a precise responsabilità, ai sensi delle normative vigenti.