ISTITUTO PROFESSIONALE DI STATO
PER I SERVIZI DI ENOGASTRONOMIA E OSPITALITA' ALBERGHIERA
- ISTITUTO ALBERGHIERO MOLFETTA -

Member of the association of European Hotel and Tourism Schools

Sede Centrale: Istituto Apicella - Corso Fornari, 1 ~ ***70056 Molfetta*** *~ Tel. 080/3345078- Fax 080/3342308*
Sede succursale: Via Giovinazzo - s.s. 16 località 1^ cala ~ ***70056 Molfetta*** *~ Tel. 080/3341896- Fax 080/3351364*
C.F. 93249230728 ~ Cod. Istituto BARH04000D Codice Univoco UF3N40
Sito web: www.alberghieromolfetta.it *e-mail* BARH04000D@istruzione.it - BARH04000D@pec.istruzione.it

LINEE GUIDA IN MATERIA DI SICUREZZA PER IL DOCENTE INCARICATO DEL TRATTAMENTO

Vengono di seguito indicate le misure operative da adottare per garantire la sicurezza dei dati personali e, in particolare, dei dati sensibili e giudiziari:
- Custodire in apposito armadio nella stanza individuata dotata di serratura come sala professori dell'edificio i seguenti documenti:
1. Registro personale
2. Certificati medici esibiti dagli alunni a giustificazione delle assenze (per il tempo strettamente necessario al loro trasferimento nei fascicoli personali in segreteria)
3. Qualunque altro documento contenente dati personali o sensibili degli alunni

Verificare la corretta funzionalità dei meccanismi di chiusura del locale, segnalando tempestivamente al responsabile di sede eventuali anomalie.
- Depositare il registro di classe, al termine delle attività didattiche giornaliere, per la sua custodia nella stanza individuata come sala professori dell'edificio.
- Seguire le istruzioni del docente responsabile dell'aula di informatica.
- Seguire le istruzioni del docente responsabile di sede nel caso di trattamento dei dati personali per fini diversi da quelli relativi ai punti 1 e 2.
- Tutte le comunicazioni indirizzate agli uffici della sede centrale, ad altro personale della scuola e al dirigente scolastico debbono essere consegnate in busta chiusa al responsabile di sede o al protocollo della sede centrale. Non è consentito, se non espressamente autorizzato, l'utilizzo del fax, della posta elettronica e dei collegamenti alla rete internet per il trattamento dei dati personali.

Per i docenti che utilizzano l'aula di informatica (nel caso di trattamento di dati personali) e per il responsabile dell'aula di informatica:

Seguire le seguenti istruzioni operative per l'utilizzo dei personal computers:
- Non lasciare dispositivi di memoria elettronica, cartelle o altri documenti a disposizione di estranei;
- 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;
- spegnere correttamente il computer al termine di ogni sessione di lavoro;
- non abbandonare la propria postazione di lavoro senza aver spento la postazione di lavoro o aver inserito uno screen saver con password;
- comunicare tempestivamente al Titolare o al Responsabile qualunque anomalia riscontrata nel funzionamento del computer;

Per i soli docenti che hanno postazioni individuali (collaboratori del dirigente):
- Scegliere una password con le seguenti caratteristiche:
  1. Originale
  2. composta da otto caratteri
  3. che contenga almeno un numero
  4. 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;
- modificare prontamente (ove possibile) la password assegnata dal custode delle credenziali;
- trascrivere su un biglietto chiuso in busta sigillata e controfirmata la nuova password e consegnarla al custode delle credenziali;
- utilizzare le seguenti regole per la posta elettronica:

1. non aprire documenti di cui non sia certa la provenienza
2. non aprire direttamente gli allegati ma salvarli su disco e controllarne il contenuto con un antivirus
3. controllare accuratamente l'indirizzo dei destinatari prima di inviare dati personali.

IL DIRIGENTE SCOLASTICO
prof. Antonio Natalicchio
(Firma autografa sostituita a mezzo stampa ai sensi dell'articolo 3, comma 2 D.lgs. 39/93)

LINEE GUIDA IN MATERIA DI SICUREZZA PER L' ASSISTENTE AMMINISTRATIVO INCARICATO DEL TRATTAMENTO

Attenersi scrupolosamente alle seguenti indicazioni per garantire la sicurezza dei dati personali e, in particolare, dei dati sensibili e giudiziari:

- Conservare sempre i dati del cui trattamento si è incaricati in apposito armadio assegnato, dotato di serratura;
- Accertarsi della corretta funzionalità dei meccanismi di chiusura dell'armadio, segnalando tempestivamente al Responsabile eventuali anomalie;
- Non consentire l'accesso alle aree in cui sono conservati dati personali su supporto cartaceo a estranei e a soggetti non autorizzati;
- Conservare i documenti ricevuti da genitori/studenti o dal personale in apposite cartelline non trasparenti;
- Consegnare al personale o ai genitori/studenti documentazione inserita in buste non trasparenti;
- Non consentire l'accesso a estranei al fax e alla stampante che contengano documenti non ancora ritirati dal personale;
- Effettuare esclusivamente copie fotostatiche di documenti per i quali si è autorizzati;
- Provvedere personalmente alla distruzione quando è necessario eliminare documenti inutilizzati;
- 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 degli studenti 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;
- Segnalare tempestivamente al Responsabile la presenza di documenti incustoditi, provvedendo temporaneamente alla loro custodia;
- 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 supporti di memoria digitale, 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 otto caratteri
  - che contenga almeno un numero
  - 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 (ove possibile) la password assegnata dal custode delle credenziali;
- trascrivere su un biglietto chiuso in busta sigillata e controfirmata la nuova password e consegnarla al custode delle credenziali;
- spegnere correttamente il computer al termine di ogni sessione di lavoro;
- non abbandonare la propria postazione di lavoro per la pausa o altri motivi senza aver spento la postazione di lavoro o aver inserito uno screen saver con password;
- comunicare tempestivamente al Titolare o al Responsabile qualunque anomalia riscontrata nel funzionamento del computer;
- 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:

- 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
- inviare messaggi di posta solo se espressamente autorizzati dal Responsabile
- controllare accuratamente l'indirizzo dei destinatari prima di inviare dati personali.

IL DIRETTORE DEI SERVIZI GENERALI E AMMINISTRATIVI
Responsabile del trattamento dati
(Firma autografa sostituita a mezzo stampa ai sensi
dell'articolo 3, comma 2 D.lgs. 39/93)

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:

(collaboratore scolastico in servizio nelle sedi e ai piani)
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:

- Registro di classe
- Certificati medici esibiti dagli alunni a giustificazione delle assenze
- Qualunque altro documento o supporto di memoria contenente dati personali o sensibili degli alunni o dei docenti

Accertarsi che al termine delle lezioni tutti i computers dell'aula di informatica siano spenti e che non siano stati lasciati incustoditi supporti di memoria, 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.

IL DIRETTORE DEI SERVIZI GENERALI E AMMINISTRATIVI
Responsabile del trattamento dati
(Firma autografa sostituita a mezzo stampa ai sensi
dell'articolo 3, comma 2 D.lgs. 39/93)