



Member of  
the association of  
European Hotel and  
Tourism Schools

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

Sede Centrale: Istituto Apicella - Corso Fornari, 1 ~ 70056 Molfetta ~ Tel. 080/3345078- Fax 080/3342308

Sede succursale: Via Giovinezza - s.s. 16 località 1<sup>a</sup> cala ~ 70056 Molfetta ~ Tel. 080/3341896- Fax 080/3351364

**C.F. 93249230728 ~ Cod. Istituto BARH04000D Codice Univoco UF3N40**

Sito web: [www.alberghieromolfetta.it](http://www.alberghieromolfetta.it) e-mail [BARH04000D@istruzione.it](mailto:BARH04000D@istruzione.it) - [BARH04000D@pec.istruzione.it](mailto:BARH04000D@pec.istruzione.it)

Istituto accreditato presso la Regione Puglia – settore Formazione Professionale – per la Formazione Superiore, per la Formazione Continua, per l'Area Svantaggio

Prot. AOO\_IPSSAR\_16517/F.PRIVACY

Molfetta, 30/12/2017

**LINEE GUIDA IN MATERIA DI SICUREZZA PER L' ASSISTENTE  
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**