



ISTITUTO COMPRENSIVO STATALE DI CARIGNANO

VIA A. TAPPI 44 - 10041 - CARIGNANO - TO

TEL. 0119692516 - Cod. Fiscale: 94067050016 - Cod. Mec.: TOIC8AQ00L

e-mail: TOIC8AQ00L@istruzione.it - TOIC8AQ00L@pec.istruzione.it

Aggiornamento al 22/4/2021 - rev. DPO

LINEE GUIDA IN MATERIA DI SICUREZZA PER L'ASSISTENTE AMMINISTRATIVO AUTORIZZATO AL TRATTAMENTO DEI DATI

Gli Assistenti amministrativi costituiscono l'unità operativa che più di altri tratta i dati personali degli alunni e del personale della scuola.

In osservanza della normativa vigente invito ad attenersi scrupolosamente alle seguenti indicazioni per garantire la sicurezza dei dati personali e, in particolare, dei dati sensibili e giudiziari.

Questo documento fornisce agli autorizzati al trattamento dati informazioni sulle loro responsabilità rispetto alla gestione ed alla sicurezza dei dati trattati dall'Istituto, in particolare riguardo:

- Integrità: le informazioni devono essere esatte, aggiornate e non alterabili;
- Riservatezza: prevenzione contro l'accesso non autorizzato delle informazioni, i trattamenti devono essere leciti e conformi alle finalità istituzionali;
- Disponibilità: il sistema deve essere protetto da interruzioni impreviste e perdite di informazioni.

Il raggiungimento di questi obiettivi richiede non solo l'utilizzo di appropriati strumenti tecnologici, ma anche gli opportuni meccanismi organizzativi; nel momento in cui le informazioni raggiungono l'utente finale, la loro protezione dipende esclusivamente da quest'ultimo, e nessun strumento tecnologico può sostituirsi al suo senso di responsabilità e al rispetto delle procedure e delle norme.

Per garantire sicurezza, e dunque integrità, esattezza e aggiornamento dei dati, nonché trattamenti leciti e conformi alle finalità della raccolta e del trattamento, gli **Assistenti Amministrativi** uniformano il loro comportamento professionale alle indicazioni sotto impartite.

- Conservare la documentazione cartacea contenente dati personali di propria competenza 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 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 alla stampante che contenga documenti non ancora ritirati dal personale;
- Effettuare esclusivamente copie fotostatiche di documenti per i quali si è autorizzati;
- Provvedere personalmente alla distruzione dei documenti quando sia necessario;
- 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;
- 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;
- Mantenere il massimo riserbo su informazioni ricevute oralmente;
- Non fornire dati e informazioni di carattere personale o sensibile per telefono se non si ha la certezza assoluta sull'identità del destinatario e la legittimità della richiesta;
- Qualora giungano richieste telefoniche di dati sensibili da parte dell'Autorità Giudiziaria o degli organi di polizia, richiedere l'identità del chiamante e quindi richiamare avendo la certezza sull'identità del richiedente; gli Assistenti Amministrativi si renderanno disponibili ad attuare la prassi anche su richiesta di docenti o collaboratori scolastici, poiché è più sicuro se l'azione è effettuata dall'Ufficio di segreteria della scuola;
- Tutte le comunicazioni indirizzate dagli uffici della sede centrale ad altro personale della scuola e al Dirigente scolastico devono essere consegnate in busta chiusa o direttamente nelle mani dell'interessato.
- Attenersi alle direttive ricevute e non effettuare operazioni per le quali non si è stati espressamente autorizzati dal Dirigente scolastico e dal DSGA.

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

- Non lasciare pendrive, cartelle o altri documenti / supporti a disposizione di estranei;
- Conservare i dati sensibili in supporti custoditi 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 otto caratteri;
 - ~ che contenga almeno un numero, una lettera maiuscola e una minuscola e possibilmente un carattere speciale (*, %, \$, ecc.);
 - ~ 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;
- spegnere correttamente il pc 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 screensaver 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: nel caso, rivolgersi al DSGA;
 - ~ 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 Dirigente Scolastico e dal DSGA;
 - ~ controllare accuratamente l'indirizzo dei destinatari prima di inviare dati personali.

LINEE GUIDA PER LA SICUREZZA DEI DATI PER IL DOCENTE AUTORIZZATO AL TRATTAMENTO DEI DATI

Questo documento fornisce agli autorizzati del trattamento informazioni sulle loro responsabilità rispetto alla gestione ed alla sicurezza dei dati trattati dall'Istituto in particolare riguardo:

- Integrità: le informazioni devono essere esatte ed aggiornate e non alterabili da incidenti o abusi;
- Riservatezza: prevenzione contro l'accesso non autorizzato delle informazioni, i trattamenti devono essere leciti e conformi alle finalità della raccolta;
- Disponibilità: il sistema deve essere protetto da interruzioni impreviste e perdite di informazioni.

Il raggiungimento di questi obiettivi richiede non solo l'utilizzo di appropriati strumenti tecnologici, ma anche gli opportuni meccanismi organizzativi; nel momento in cui le informazioni raggiungono l'utente finale, la loro protezione dipende esclusivamente da quest'ultimo, e nessun strumento tecnologico può sostituirsi al suo senso di responsabilità e al rispetto delle procedure e delle norme. Autorizzato al trattamento dei dati sottoelencati è individuato **l'intero corpo insegnante**. Pertanto **ogni docente**, nel momento in cui è assegnato a far parte del corpo insegnante, diventa automaticamente incaricato di tali trattamenti e riceve dal Titolare o dal Responsabile del trattamento le presenti istruzioni operative scritte.

Per garantire sicurezza, e dunque integrità, esattezza e aggiornamento dei dati, nonché trattamenti leciti e conformi alle finalità della raccolta, i docenti uniformano il loro comportamento professionale alle indicazioni sotto impartite.

Al fine di garantire il diritto alla protezione dei dati e alla riservatezza, nel trattamento dei dati i docenti sono tenuti a:

- a. Procedere alla raccolta dei dati con massima cura verificando l'esattezza dei dati stessi;
- b. Procedere all'aggiornamento dei dati, ove necessario, qualora vengano svolte operazioni dinamiche di trattamento.

Inoltre, i docenti si adoperano per:

- a. Prevenire la diffusione illecita dei dati personali e sensibili, avendo cura di accedere ai soli dati la cui conoscenza sia strettamente necessaria per lo svolgimento delle funzioni e dei compiti affidati e per le finalità di cui al provvedimento di incarico.
- b. Custodire i dati trattati in forma cartacea avendo cura di:
 - i. Conservare i documenti o atti che contengono dati personali o sensibili o giudiziari in contenitori chiusi a chiave;
 - ii. Distruggere o comunque rendere illeggibili, prima di essere eliminati o cestinati, i documenti cartacei non più utilizzati;
 - iii. Non lasciare fogli, cartelle o altri supporti a disposizione di estranei;
 - iv. Custodire in archivio sicuro gli elaborati degli studenti nel caso contenessero dati particolari. Se nel contenuto è ravvisabile un dato sensibile l'elaborato deve essere riposto in busta chiusa;
 - v. Non lasciare abbandonati elenchi che riportano dati di alunni; in occasione delle uscite didattiche e/o delle gite, in caso di richiesta di elenchi da parte di terzi, verificare la congruità della richiesta e, salvo eccezionali casi espressamente autorizzati, che i suddetti elenchi non riportino dati sensibili.
- c. Custodire i dati trattati elettronicamente avendo cura di seguire il Regolamento per l'utilizzo dei sistemi informatici, e nello specifico avendo cura di:
 - i. Aggiornare quotidianamente il registro elettronico custodendo accuratamente le credenziali d'accesso;
 - ii. Verificare che l'antivirus sia aggiornato prima di operare con pendrive che contengono dati sensibili e non per evitare la perdita o la diffusione.

- d. Prevenire la comunicazione illecita di dati personali avendo cura di:
- i. Mantenere il riserbo su informazioni ricevute oralmente;
 - ii. Non fornire dati e informazioni di carattere sensibile al telefono se non si ha la certezza assoluta sull'identità del destinatario;
 - iii. Qualora giungano richieste telefoniche di dati sensibili da parte dell'Autorità Giudiziaria o degli organi di polizia, richiedere l'identità del chiamante e quindi richiamare avendo la certezza sull'identità del richiedente; meglio se l'azione è effettuata dall'ufficio di segreteria della scuola;
 - iv. Tutte le comunicazioni indirizzate agli uffici della sede centrale, ad altro personale della scuola e al Dirigente scolastico devono essere consegnate in busta chiusa o direttamente nelle mani dell'interessato.
- e Al fine di monitorare e valutare l'efficacia del piano di protezione dei dati personali è necessario comunicare per scritto al Titolare del trattamento eventuali difformità dei dati trattati.

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 devices informatici;

- Non lasciare pendrive, cartelle, supporti 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;
- Scegliere una password con le seguenti caratteristiche:
 - Originale;
 - composta da almeno otto caratteri;
 - che contenga almeno un numero, una lettera maiuscola e una minuscola e possibilmente un carattere speciale (*, %, \$, ecc.);
 - 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.
- 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;
- 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;
 - controllare accuratamente l'indirizzo del destinatario prima di inviare dati personali.

LINEE GUIDA IN MATERIA DI SICUREZZA PER IL COLLABORATORE SCOLASTICO AUTORIZZATO AL TRATTAMENTO

Questo documento fornisce agli autorizzati del trattamento informazioni sulle loro responsabilità rispetto alla gestione ed alla sicurezza dei dati trattati dall'Istituto in particolare riguardo:

- Integrità: le informazioni devono essere esatte ed aggiornate e non alterabili da incidenti o abusi;
- Riservatezza: prevenzione contro l'accesso non autorizzato delle informazioni, i trattamenti devono essere leciti e conformi alle finalità della raccolta;
- Disponibilità: il sistema deve essere protetto da interruzioni impreviste e perdite di informazioni.

Il raggiungimento di questi obiettivi richiede non solo l'utilizzo di appropriati strumenti tecnologici, ma anche gli opportuni meccanismi organizzativi; nel momento in cui le informazioni raggiungono l'utente finale, la loro protezione dipende esclusivamente da quest'ultimo, e nessun strumento tecnologico può sostituirsi al suo senso di responsabilità e al rispetto delle procedure e delle norme. Autorizzato del trattamento dei dati sotto elencati è l'unità organizzativa denominata "**Collaboratori scolastici**". Pertanto ogni unità di personale, nel momento in cui è assegnato a tale ruolo diventa automaticamente autorizzato al trattamento e riceve dal Titolare o dal Responsabile del trattamento le presenti istruzioni scritte.

Per garantire sicurezza cioè integrità, esattezza e aggiornamento dei dati, nonché trattamenti leciti e conformi alle finalità della raccolta i Collaboratori Scolastici uniformano il loro comportamento professionale alle indicazioni sotto impartite.

- al fine di garantire il diritto alla protezione dei dati personali e la riservatezza, i collaboratori scolastici nel trattamento dei dati sono tenuti a:
 - procedere alla raccolta dei dati con massima cura verificando l'esattezza dei dati stessi;
 - procedere all'aggiornamento dei dati, ove necessario, qualora vengano svolte operazioni dinamiche di trattamento.
- i collaboratori scolastici si occupano inoltre di:
 - prevenire la diffusione illecita dei dati personali e sensibili, avendo cura di:
 - accedere ai soli dati la cui conoscenza sia strettamente necessaria per lo svolgimento delle funzioni e dei compiti affidati;
 - impedire l'intrusione nei locali che sono stati loro affidati in custodia da parte di persone non autorizzate;
 - impedire il danneggiamento, la manomissione, la sottrazione, la distruzione o la copia di dati nei locali che sono stati affidati loro in custodia da parte di persone non autorizzate;
 - Custodire i dati trattati con mezzi non elettronici avendo cura di:
 - Conservare i documenti o atti che contengono dati personali o sensibili o giudiziari in contenitori chiusi a chiave o negli appositi archivi;
 - Distruggere o comunque rendere illeggibili, prima di essere eliminati o cestinati, i documenti cartacei non più utilizzati;
 - Non lasciare fogli, pendrive, cartelle o altro supporti a disposizione di estranei;
 - Non lasciare incustoditi i registri didattici eventualmente ricevuti in custodia temporanea, nonché inibirne la consultazione a terzi non autorizzati;
 - Non lasciare abbandonati elenchi che riportano dati di alunni qualora siano consegnati da altri operatori della scuola per particolari esigenze.
 - Prevenire la comunicazione illecita di dati personali avendo cura di:
 - Mantenere il massimo riserbo su informazioni ricevute oralmente;
 - Non fornire dati e informazioni di carattere personale o sensibile per telefono se non si ha la certezza assoluta sull'identità del destinatario e la legittimità della richiesta;

- Qualora giungano richieste telefoniche di dati sensibili da parte dell'Autorità Giudiziaria o degli organi di polizia, richiedere l'identità del chiamante e riferire al Dirigente Scolastico, al DSGA o all'ufficio interessato.
 - Tutte le comunicazioni indirizzate agli uffici della sede centrale, ad altro personale della scuola e al Dirigente scolastico devono essere consegnate in busta chiusa o direttamente nelle mani dell'interessato.
- al fine di monitorare e valutare l'efficacia del piano di protezione dei dati personali è necessario comunicare per scritto al Titolare del trattamento eventuali difformità dei dati trattati.

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 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 pc dell'**aula di informatica** siano spenti e che non siano stati lasciati incustoditi pendrive, cartelle o altri supporti, in caso contrario segnalarne tempestivamente la presenza al Responsabile di laboratorio o al DSGA, 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.

Collaboratore scolastico in servizio negli uffici di segreteria.

- 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 DSGA 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 degli uffici siano state depositate negli appositi contenitori.

Attenersi alle direttive ricevute e non effettuare operazioni per le quali non si sia stati espressamente autorizzati dal Dirigente scolastico e dal DSGA.

IL DIRIGENTE SCOLASTICO
dott.ssa Rosa FORLENZA