



ISTITUTO PROFESSIONALE DI STATO  
“ARMANDO PEROTTI”

**LINEE GUIDA IN MATERIA DI SICUREZZA PER L' ASSISTENTE TECNICO AUTORIZZATO AL TRATTAMENTO**

Vengono di seguito riportate le norme cui dovrà attenersi il personale Assistente tecnico autorizzato al trattamento dei dati personali. Ulteriori informazioni sulla modalità del trattamento dei dati e sulle misure di sicurezza adottate sono contenute nel registro dei trattamenti.

- Controllare e custodire gli atti e i documenti contenenti dati personali in modo da assicurarne l'integrità e la riservatezza;
- Conservare sempre i dati del cui trattamento si è incaricati in apposito armadio assegnato;
- Accertarsi della corretta funzionalità dei meccanismi di chiusura dell'armadio, segnalando tempestivamente eventuali anomalie;
- Prima di procedere alla raccolta e al trattamento dei dati fornire sempre l'informativa all'interessato o alla persona presso cui si raccolgono i dati;
- Consegnare, quando necessario, il modulo per il consenso da parte dell'interessato. Ricevere quindi il modello opportunamente firmato da parte dell'interessato o di chi lo rappresenta;
- Occorre procedere alla raccolta dei dati con la massima cura verificando l'esattezza dei dati stessi;
- Si può accedere ai soli dati personali, oggetto di trattamento, 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;
- I documenti o atti che contengono dati sensibili o giudiziari devono essere conservati in archivi (ad esempio stanze, armadi, schedari, contenitori in genere) chiusi a chiave;
- Non fornire telefonicamente o a mezzo fax dati e informazioni relativi a terzi, senza una specifica autorizzazione del titolare;
- Qualora giungano richieste telefoniche di dati sensibili da parte dell'Autorità Giudiziaria o degli organi di polizia si deve richiedere l'identità del chiamante. Quindi si provvederà a richiamare avendo così la certezza sull'identità del richiedente;
- Non fornire, anche telefonicamente o per mail, dati e informazioni ai diretti interessati senza avere la certezza della loro identità;
- Nella comunicazione di dati sensibili adottare sempre procedure che permettano di garantire la sicurezza e la riservatezza delle informazioni anche mediante tecniche di anonimizzazione e di pseudonimizzazione;
- I documenti cartacei non più utilizzati, specie se sensibili, devono essere distrutti o comunque resi illeggibili, prima di essere eliminati o cestinati;
- 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;



ISTITUTO PROFESSIONALE DI STATO

“ARMANDO PEROTTI”

- Non consentire l'accesso a estranei ad aree in cui sono custoditi documenti cartacei o contengono supporti informatici di memorizzazione;
- Effettuare esclusivamente copie fotostatiche o su supporto informatico 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 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 Titolare.

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

- Per l'accesso al sistema informatico utilizzare le credenziali di accesso ricevute;
- Adottare le necessarie cautele per assicurare la segretezza della parola chiave e la diligente custodia di ogni altro dispositivo di autenticazione informatica (badge, schede magnetiche, chiavi USB, etc.);
- È fatto divieto di comunicare a qualunque altro incaricato le proprie credenziali di accesso al sistema informatico;
- La parola chiave deve essere modificata almeno ogni tre mesi;
- Tutte le volte che si abbandoni la propria postazione di lavoro i pc e/o i terminali devono essere posti in condizione di non essere utilizzati da estranei. In particolare si raccomanda di chiudere tutte le applicazioni in uso e di porre un blocco del sistema mediante password;
- Spegnerne sempre il PC alla fine della giornata lavorativa o in caso di assenze prolungate dalla postazione di lavoro;
- Qualora si dovessero riscontrare difformità dei dati trattati o nel funzionamento degli elaboratori occorre darne immediata comunicazione al titolare del trattamento;
- Utilizzare l'antivirus per la verifica di ogni documento trattato o di qualunque file scaricato da Internet;
- Utilizzare sempre l'antivirus per verificare il contenuto di qualunque supporto di memorizzazione sospetto;
- Aggiornare con frequenza l'antivirus;
- Utilizzare esclusivamente le piattaforme identificate dalla scuola come sicure e nominate dalla stessa responsabili del trattamento, specie qualora si renda necessario effettuare delle attività lavorative a distanza, come previsto dalle modalità organizzative della scuola e dalla normative vigente;



ISTITUTO PROFESSIONALE DI STATO

“ARMANDO PEROTTI”

- Verificare sempre la corretta modifica e/o cancellazione di dati su documenti, cartelle o informazioni condivise alle quali si abbia accesso nell'esercizio delle proprie funzioni (double check), al fine di evitare modifiche o cancellazioni indesiderate che possano arrecare danno agli interessati o limitare le possibilità di lavoro di colleghi.
- Nelle comunicazioni via mail assicurarsi di non usare impropriamente il campo CC con la conseguenza di portare indebitamente a conoscenza di tutti i destinatari del messaggio i relativi indirizzi email (usare invece il campo CCN se è necessario tenere riservati gli indirizzi email di coloro che sono coinvolti nella comunicazione).

#### **Regole per la scelta delle parole chiave**

- Usare una parola chiave di almeno dodici caratteri;
- La parola chiave non deve contenere riferimenti facilmente riconducibili all'incaricato (come per esempio nome, cognome, data di nascita, numeri di telefono, etc. propri o dei propri familiari);
- Usare una combinazione di caratteri alfabetici e numerici, meglio se contenente almeno un segno di interpunzione o un carattere speciale;
- Conservare con cura la parola chiave evitando di trascriverla su fogli posti in vista in prossimità del PC o sulla rubrica dell'ufficio.

Si precisa che il titolare è sempre e comunque responsabile della mancata esecuzione degli adempimenti previsti dal D.lgs. n.196/2003 e del Regolamento UE 2016/679. Tuttavia le responsabilità, per l'inosservanza delle istruzioni impartite dal Titolare e/o dai responsabili, possono riguardare anche gli incaricati, che non rispettino o non adottino le misure necessarie.

***IL DIRIGENTE SCOLASTICO***

***Prof. Leonardo CASTELLANA***

Firma autografa sostituita da indicazioni a mezzo stampa, ai sensi dell'art. 3, comma 2, del d.lgs. n.39/1993



ISTITUTO PROFESSIONALE DI STATO  
“ARMANDO PEROTTI”



**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 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 ed 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 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 sia stati espressamente autorizzati dal Titolare;
- Identificare e verificare l'autorizzazione all'accesso ai locali dei soggetti ammessi dopo l'orario di chiusura.

**Collaboratore scolastico 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 sede e provvedendo temporaneamente alla loro custodia:

- Registro personale dei docenti;
- Registro di classe;
- Qualunque altro documento contenente dati personali o sensibili degli alunni o dei docenti
- Registro personale dei docenti;
- 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 dell'aula di informatica siano spenti e che non siano stati lasciati incustoditi supporti di memoria, in caso contrario segnalarne tempestivamente la presenza al responsabile di laboratorio o di sede provvedendo temporaneamente alla loro custodia;



ISTITUTO PROFESSIONALE DI STATO  
“ARMANDO PEROTTI”



- 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.

***IL DIRIGENTE SCOLASTICO***

***Prof. Leonardo CASTELLANA***

Firma autografa sostituita da indicazioni a mezzo stampa, ai sensi  
dell'art. 3, comma 2, del d.lgs. n.39/1993



ISTITUTO PROFESSIONALE DI STATO

“ARMANDO PEROTTI”

### LINEE GUIDA IN MATERIA DI SICUREZZA PER IL PERSONALE AMMINISTRATIVO AUTORIZZATO AL TRATTAMENTO

Vengono di seguito riportate le norme cui dovrà attenersi il personale amministrativo autorizzato al trattamento dei dati personali. Ulteriori informazioni sulla modalità del trattamento dei dati e sulle misure di sicurezza adottate sono contenute nel registro dei trattamenti.

- Controllare e custodire gli atti e i documenti contenenti dati personali in modo da assicurarne l'integrità e la riservatezza;
- Conservare sempre i dati del cui trattamento si è incaricati in apposito armadio assegnato;
- Accertarsi della corretta funzionalità dei meccanismi di chiusura dell'armadio, segnalando tempestivamente eventuali anomalie;
- Prima di procedere alla raccolta e al trattamento dei dati fornire sempre l'informativa all'interessato o alla persona presso cui si raccolgono i dati;
- Consegnare, quando necessario, il modulo per il consenso da parte dell'interessato. Ricevere quindi il modello opportunamente firmato da parte dell'interessato o di chi lo rappresenta;
- Occorre procedere alla raccolta dei dati con la massima cura verificando l'esattezza dei dati stessi;
- Si può accedere ai soli dati personali, oggetto di trattamento, 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;
- I documenti o atti che contengono dati sensibili o giudiziari devono essere conservati in archivi (ad esempio stanze, armadi, schedari, contenitori in genere) chiusi a chiave;
- Non fornire telefonicamente o a mezzo fax dati e informazioni relativi a terzi, senza una specifica autorizzazione del titolare;
- Qualora giungano richieste telefoniche di dati sensibili da parte dell'Autorità Giudiziaria o degli organi di polizia si deve richiedere l'identità del chiamante. Quindi si provvederà a richiamare avendo così la certezza sull'identità del richiedente;
- Non fornire, anche telefonicamente o per mail, dati e informazioni ai diretti interessati senza avere la certezza della loro identità;
- Nella comunicazione di dati sensibili adottare sempre procedure che permettano di garantire la sicurezza e la riservatezza delle informazioni anche mediante tecniche di anonimizzazione e di pseudonimizzazione;
- I documenti cartacei non più utilizzati, specie se sensibili, devono essere distrutti o comunque resi illeggibili, prima di essere eliminati o cestinati;
- 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;



ISTITUTO PROFESSIONALE DI STATO

“ARMANDO PEROTTI”



- Consegnare al personale o ai genitori/studenti documentazione inserita in buste non trasparenti;
- Non consentire l'accesso a estranei ad aree in cui sono custoditi documenti cartacei o contengano supporti informatici di memorizzazione;
- Effettuare esclusivamente copie fotostatiche o su supporto informatico 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 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 Titolare.

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

- Per l'accesso al sistema informatico utilizzare le credenziali di accesso ricevute;
- Adottare le necessarie cautele per assicurare la segretezza della parola chiave e la diligente custodia di ogni altro dispositivo di autenticazione informatica (badge, schede magnetiche, chiavi USB, etc.);
- È fatto divieto di comunicare a qualunque altro incaricato le proprie credenziali di accesso al sistema informatico;
- La parola chiave deve essere modificata almeno ogni tre mesi;
- Tutte le volte che si abbandoni la propria postazione di lavoro i pc e/o i terminali devono essere posti in condizione di non essere utilizzati da estranei. In particolare si raccomanda di chiudere tutte le applicazioni in uso e di porre un blocco del sistema mediante password;
- Spegnerne sempre il PC alla fine della giornata lavorativa o in caso di assenze prolungate dalla postazione di lavoro;
- Qualora si dovessero riscontrare difformità dei dati trattati o nel funzionamento degli elaboratori occorre darne immediata comunicazione al titolare del trattamento;
- Utilizzare l'antivirus per la verifica di ogni documento trattato o di qualunque file scaricato da Internet;
- Utilizzare sempre l'antivirus per verificare il contenuto di qualunque supporto di memorizzazione sospetto;
- Aggiornare con frequenza l'antivirus;



ISTITUTO PROFESSIONALE DI STATO

“ARMANDO PEROTTI”

- Utilizzare esclusivamente le piattaforme identificate dalla scuola come sicure e nominate dalla stessa responsabili del trattamento, specie qualora si renda necessario effettuare delle attività lavorative a distanza, come previsto dalle modalità organizzative della scuola e dalla normative vigente;
- Verificare sempre la corretta modifica e/o cancellazione di dati su documenti, cartelle o informazioni condivise alle quali si abbia accesso nell’esercizio delle proprie funzioni (double check), al fine di evitare modifiche o cancellazioni indesiderate che possano arrecare danno agli interessati o limitare le possibilità di lavoro di colleghi.
- Nelle comunicazioni via mail assicurarsi di non usare impropriamente il campo CC con la conseguenza di portare indebitamente a conoscenza di tutti i destinatari del messaggio i relativi indirizzi email (usare invece il campo CCN se è necessario tenere riservati gli indirizzi email di coloro che sono coinvolti nella comunicazione).

#### **Regole per la scelta delle parole chiave**

- Usare una parola chiave di almeno dodici caratteri;
- La parola chiave non deve contenere riferimenti facilmente riconducibili all’incaricato (come per esempio nome, cognome, data di nascita, numeri di telefono, etc. propri o dei propri familiari);
- Usare una combinazione di caratteri alfabetici e numerici, meglio se contenente almeno un segno di interpunzione o un carattere speciale;
- Conservare con cura la parola chiave evitando di trascriverla su fogli posti in vista in prossimità del PC o sulla rubrica dell’ufficio.

Si precisa che il titolare è sempre e comunque responsabile della mancata esecuzione degli adempimenti previsti dal D.lgs. n.196/2003 e del Regolamento UE 2016/679. Tuttavia le responsabilità, per l’inosservanza delle istruzioni impartite dal Titolare e/o dai responsabili, possono riguardare anche gli incaricati, che non rispettino o non adottino le misure necessarie.

***IL DIRIGENTE SCOLASTICO***

***Prof. Leonardo CASTELLANA***

Firma autografa sostituita da indicazioni a mezzo stampa, ai sensi dell'art. 3, comma 2, del d.lgs. n.39/1993