



MINISTERO DELL' ISTRUZIONE E DEL MERITO  
ISTITUTO COMPRENSIVO BONO

Via Tirso, 07011 Bono Tel. 079 790110- [WWW.ics-bono.edu.it](http://WWW.ics-bono.edu.it)  
e.mail:ssic820006@istruzione.it – Pec: ssic820006@pec.istruzione.it  
Cod Univocolpa: UFRWLA – Cod.IPA istsc\_ssic820006  
C.F. 81000530907

All' Assistente Tecnico

I.C. Bono - Sede

**Oggetto:** Protezione dei dati personali – Regolamento UE 2016/679. Designazione in qualità di soggetto “autorizzato al trattamento di dati personali” dei componenti dell’unità organizzativa “AssistentieTecnico”.

**IL DIRIGENTE SCOLASTICO**

**VISTO** il Regolamento UE 2016/679 (GDPR), con particolare riguardo agli artt. 4 (n. 10), 24, 28, 29 e 32;

**VISTO** il Decreto Legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali), come novellato dal D.Lgs. 101/2018, e in particolare l’art. 2-quaterdecies (Attribuzione di funzioni e compiti a soggetti designati), nonché gli artt. 2-sexies e 2-octies;

**VISTO** il Codice dell’Amministrazione Digitale (D.Lgs. 82/2005), che impone la formazione e la gestione dei documenti amministrativi in formato elettronico;

**CONSIDERATO** che questo Istituto è titolare del trattamento dei dati personali di alunni, genitori, personale dipendente, fornitori e di qualunque altro soggetto che abbia rapporti con l’Istituto e che a questo conferisca, volontariamente o per obbligo, propri dati personali;

**CONSIDERATO** che la titolarità del trattamento è esercitata dallo scrivente Dirigente, in qualità di legale rappresentante pro-tempore dell’Istituto;

**CONSIDERATO** che gli assistenti tecnici in servizio trattano dati personali nello svolgimento delle proprie mansioni, in particolare in occasione degli interventi di assistenza e manutenzione sui sistemi informatici dell’amministrazione;

**DETERMINA**

1. di designare l’unità organizzativa ASSISTENTI TECNICI, cui appartengono tutti i dipendenti aventi il profilo di Assistente Tecnico, quale unità **autorizzata al trattamento** dei dati personali;
2. di dare atto che ogni dipendente che cessa di far parte di questa unità organizzativa cessa automaticamente dalla funzione di soggetto autorizzato al trattamento, che ogni nuovo dipendente che vi entra assume automaticamente la funzione di soggetto autorizzato al trattamento e che, in un determinato momento, l’elenco dei soggetti autorizzati corrisponde all’elenco dei dipendenti validamente in servizio che ne fanno parte;
3. di autorizzare i componenti di questa unità organizzativa a trattare i dati personali con cui entrino in contatto nell’ambito dell’espletamento dell’attività di loro competenza o contenuti nelle banche dati, negli archivi cartacei anche frammentari, nelle memorie dei computer, negli archivi della scuola e nelle piattaforme cloud messe a disposizione dall’amministrazione, raccolti per l’assolvimento delle finalità istituzionali;

4. di autorizzare l'unità organizzativa alle operazioni di raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, modifica, comunicazione (nei soli casi autorizzati dal titolare), selezione ed estrazione di dati connesse alle attività di propria competenza. L'accesso ai dati personali è consentito solo per lo svolgimento di una specifica mansione o incarico ricevuto, in assenza del quale l'appartenenza all'unità organizzativa non autorizza all'accesso ai dati personali;
5. di autorizzare l'unità organizzativa a trattare i dati appartenenti a **categorie particolari** (art. 9 del Regolamento) e i dati relativi a **condanne penali e reati** (art. 10 del Regolamento) con cui vengano a contatto durante l'attività di loro competenza, nei limiti di quanto previsto dalla normativa vigente. Il trattamento di tali dati trova la propria base di liceità negli artt. 2-sexies e 2-octies del Codice (motivi di interesse pubblico rilevante) e avviene nel rispetto delle tipologie di dati e operazioni individuate dal D.M. 7 dicembre 2006, n. 305, tuttora applicabile in via transitoria ai sensi dell'art. 22, comma 9, del D.Lgs. 101/2018, pubblicato nel sito web istituzionale in Amministrazione Trasparente – sezione Disposizioni generali / Atti generali;  
  
[https://www.trasparenzascuole.it/Public/AmministrazioneTrasparenteV3.aspx?Customer\\_id=93f38237-84d6-4e22-91b7-39bd7815efc1&PID=897ce888-55cc-429a-8a8c-4055387b1ee7](https://www.trasparenzascuole.it/Public/AmministrazioneTrasparenteV3.aspx?Customer_id=93f38237-84d6-4e22-91b7-39bd7815efc1&PID=897ce888-55cc-429a-8a8c-4055387b1ee7)
6. di dare atto che l'appartenenza all'unità organizzativa ASSISTENTI TECNICI non autorizza all'accesso indiscriminato ai dati personali e alle categorie particolari di dati trattati dall'amministrazione, che dovrà invece essere autorizzato per ogni singolo soggetto in base alle mansioni da svolgere e all'incarico ricevuto;
7. fermi restando gli obblighi e le responsabilità civili e penali dei dipendenti pubblici, di disporre sotto vincolo disciplinare l'obbligo tassativo di attenersi alle istruzioni che seguono per tutti i componenti dell'unità organizzativa.

**Per tutti gli appartenenti all'unità organizzativa ASSISTENTI TECNICI sono fornite le istruzioni operative che seguono:**

1. il trattamento dei dati personali è consentito soltanto nell'ambito dello svolgimento delle funzioni istituzionali della scuola e deve avvenire secondo correttezza e liceità, nel rispetto del D.Lgs. 196/2003 e del Regolamento UE 2016/679; i dati devono essere esatti, aggiornati, pertinenti e non eccedenti;
2. è vietata qualsiasi forma di diffusione e comunicazione dei dati personali che non sia strettamente funzionale ai compiti affidati e comunque autorizzata dal titolare; l'obbligo di riservatezza permane anche oltre il limite temporale dell'incarico;
3. gli atti e i documenti contenenti dati personali non devono mai essere lasciati incustoditi; al termine del trattamento vanno riposti in contenitori muniti di serratura, la cui chiave va custodita, e non possono essere portati fuori sede né riprodotti senza espressa autorizzazione del titolare;
4. custodire con cura le proprie credenziali di autenticazione: sono personali, non possono essere rivelate a terzi e, in caso di smarrimento o furto, ne va data comunicazione immediata al titolare; utilizzare, ove disponibile, l'autenticazione a più fattori (MFA);
5. gli eventuali supporti rimovibili contenenti dati personali devono essere attentamente custoditi per prevenire accessi non autorizzati;
6. l'accesso a categorie particolari di dati o a dati relativi a condanne penali e reati è permesso solo alle persone autorizzate ed è soggetto a costante controllo;
7. nelle comunicazioni in forma elettronica seguire procedure che garantiscano la riservatezza dei dati trasmessi, richiamati o citati;
8. segnalare senza ritardo al Dirigente Scolastico e, per il suo tramite, al Responsabile della Protezione dei Dati qualunque violazione o sospetta violazione dei dati personali – anche rilevata nel corso degli interventi tecnici (accessi non autorizzati, perdita, alterazione o divulgazione di dati) – ai fini degli adempimenti di cui agli artt. 33 e 34 del Regolamento.

9. **Utilizzo di strumenti di intelligenza artificiale.** Nell'utilizzo di strumenti basati sull'intelligenza artificiale per attività amministrative (redazione, riformulazione o sintesi di documenti) è vietato inserire dati personali – a maggior ragione se relativi a categorie particolari o a minori – nei prompt forniti a strumenti di intelligenza artificiale a meno che ciò sia consentito in un caso d'uso esplicitamente ammesso dall'amministrazione; possono essere utilizzati esclusivamente gli strumenti individuati e autorizzati dall'Istituto e il testo prodotto dall'IA deve sempre essere riletto e validato da un operatore. Chiunque utilizzi strumenti IA deve partecipare alle attività di alfabetizzazione in materia di intelligenza artificiale organizzate dall'Istituto, in adempimento dell'obbligo di cui all'art. 4 del Regolamento (UE) 2024/1689;

**In particolare, in occasione degli interventi di assistenza e manutenzione sui dispositivi dell'amministrazione, l'assistente tecnico deve:**

- evitare qualunque accesso ai dati personali presenti nei dispositivi, a meno che non sia tecnicamente necessario allo svolgimento del compito ricevuto;
- effettuare preventivamente la copia di sicurezza dei dati ogni qualvolta l'intervento comporti il rischio della loro perdita;
- garantire la riservatezza e l'integrità dei dati personali trattati nello svolgimento dell'attività di assistenza e manutenzione;
- non utilizzare i dati cui abbia accesso per finalità incompatibili con quelle relative al proprio profilo.

Il titolare precisa che tutte le presenti istruzioni sono vincolanti e obbligatorie e che qualunque violazione può dare luogo a specifici provvedimenti disciplinari, oltre a precise responsabilità, ai sensi del D.Lgs. 196/2003 e del Regolamento UE 2016/679. L'autorizzazione al trattamento si intende automaticamente revocata alla data di cessazione del rapporto di lavoro con questa istituzione scolastica, per trasferimento ad altra istituzione o per altra causa.

Allegati: Linee Guida

**F.to: Pierpaolo Pinna Dirigente**  
(titolare del trattamento)

## **LINEE GUIDA IN MATERIA DI SICUREZZA PER IL TRATTAMENTO DEI DATI PERSONALI**

### **ASSISTENTI TECNICI AUTORIZZATI AL TRATTAMENTO**

*Le presenti linee guida descrivono le misure operative che gli assistenti tecnici, in qualità di soggetti autorizzati al trattamento, sono chiamati ad adottare per garantire la sicurezza dei dati personali degli interessati, ai sensi del Regolamento UE 2016/679 e del D.Lgs. 196/2003 (novellato dal D.Lgs. 101/2018).*

#### **Definizioni**

**Trattamento:** *qualunque operazione, svolta con o senza l'ausilio di mezzi elettronici o comunque automatizzati, concernente la raccolta, registrazione, organizzazione, conservazione, elaborazione, modificazione, selezione, estrazione, raffronto, utilizzo, interconnessione, blocco, comunicazione, diffusione, cancellazione e distruzione dei dati (art. 4 del Regolamento).*

**Persona autorizzata al trattamento:** *chiunque agisca sotto l'autorità del titolare o del responsabile del trattamento (art. 29 del Regolamento; art. 2-quaterdecies del Codice). È la figura che il previgente Codice definiva "incaricato".*

**Violazione dei dati personali (data breach):** *la violazione di sicurezza che comporta, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati (art. 4 del Regolamento).*

#### **Misure operative generali**

*Nello svolgimento delle proprie mansioni l'assistente tecnico, in qualità di soggetto autorizzato al trattamento, dovrà:*

- trattare i dati personali in modo lecito e corretto, per scopi determinati, espliciti e legittimi e per finalità compatibili con quelle del proprio profilo, verificando che siano esatti, aggiornati, pertinenti, completi e non eccedenti;*
- conservare i dati in forma che consenta l'identificazione dell'interessato per un tempo non superiore a quello necessario agli scopi del trattamento;*
- comunicare, diffondere o trasferire all'esterno dati personali relativi a terzi esclusivamente ai soggetti autorizzati e nel rispetto delle istruzioni ricevute; al di fuori dell'ambito lavorativo astenersi dal comunicare a terzi qualsivoglia dato personale;*
- segnalare senza ritardo al Dirigente Scolastico e, per il suo tramite, al Responsabile della Protezione dei Dati (nonché all'eventuale referente privacy) ogni circostanza idonea a determinare una violazione dei dati personali, ai fini degli adempimenti di cui agli artt. 33 e 34 del Regolamento;*
- non fornire telefonicamente o con altri mezzi dati e informazioni relativi a terzi senza una specifica autorizzazione del titolare e senza il previo accertamento dell'identità del richiedente;*
- non lasciare a disposizione di estranei, e non abbandonare la postazione senza aver custodito in luogo sicuro, documenti o supporti di memorizzazione contenenti dati personali, categorie particolari di dati o dati relativi a condanne penali e reati;*
- nel caso di registri cartacei, al termine delle attività giornaliere riporli in armadio o cassetto dotato di serratura nel locale adibito alla loro custodia, o consegnarli al collaboratore scolastico incaricato;*
- accertarsi della corretta distruzione (tramite distruggi-documenti) dei documenti contenenti dati personali, particolari o giudiziari non più utilizzati o superflui, ed effettuare copie fotostatiche di tali documenti esclusivamente previa autorizzazione, prevenendone perdita, distruzione o danni durante duplicazione e trasporto;*
- provvedere alla chiusura dei locali non utilizzati in caso di assenza del personale e verificare la corretta funzionalità dei meccanismi di chiusura degli armadi che custodiscono dati personali, segnalando tempestivamente al responsabile di sede eventuali anomalie.*

### **Misure operative specifiche per l'uso delle tecnologie informatiche**

- utilizzare password di almeno dodici caratteri (maiuscole, minuscole, numeri e caratteri speciali), non facilmente intuibili, non riconducibili alla propria persona e non riutilizzate su altri servizi; utilizzare, ove disponibile, l'autenticazione a più fattori (MFA);
- conservare accuratamente le proprie password e non comunicarle a terzi per alcun motivo; modificare la password in caso di sospetta compromissione o su indicazione dell'amministratore di sistema (non è richiesta una rotazione periodica prefissata, in coerenza con le indicazioni AgID);
- prima di abbandonare la postazione, anche temporaneamente, effettuare il log-off dai sistemi e dalle piattaforme o attivare il blocco schermo protetto da password; al termine della sessione di lavoro spegnere i dispositivi;
- non immettere in strumenti di intelligenza artificiale generalisti non contrattualizzati dalla scuola dati personali eventualmente incontrati nel corso dell'attività (a maggior ragione se relativi a categorie particolari o a minori) e utilizzare esclusivamente gli strumenti di IA individuati e autorizzati dall'Istituto;
- nella comunicazione con alunni e genitori utilizzare esclusivamente le piattaforme informatiche messe a disposizione dall'Istituto; è vietato l'uso dei social network;
- nell'uso della posta elettronica non aprire allegati di provenienza incerta e controllare accuratamente gli indirizzi dei destinatari prima di inviare messaggi contenenti dati personali;
- per la creazione, lettura o modifica di documenti in locale contenenti dati personali di alunni o genitori, utilizzare esclusivamente le apparecchiature informatiche fornite dalla scuola, in linea con le Misure minime di sicurezza ICT emanate da AgID.

### **Disposizioni per la gestione degli apparati (ove assegnato l'incarico di gestore dei sistemi)**

All'assistente tecnico cui sia assegnato l'incarico di gestore dei sistemi informatici di un laboratorio o dell'intero istituto si applicano, in aggiunta, le seguenti misure:

- gestire le utenze e i profili di accesso secondo il principio del minimo privilegio, attivandoli e disattivandoli tempestivamente in raccordo con la segreteria;
- assicurare l'aggiornamento dei sistemi operativi e degli applicativi (patch di sicurezza) e il corretto funzionamento delle soluzioni di protezione (endpoint);
- effettuare e verificare periodicamente i backup dei dati e testarne il ripristino;
- mantenere un inventario aggiornato dei dispositivi e curare la cancellazione sicura dei dati sui dispositivi dismessi;
- segnalare tempestivamente al Dirigente e al DPO ogni incidente di sicurezza o anomalia rilevata sui sistemi.

Si precisa che il titolare è sempre e comunque responsabile della corretta esecuzione degli adempimenti previsti dal D.Lgs. 196/2003 e dal Regolamento UE 2016/679. Tuttavia, le responsabilità per l'inosservanza delle istruzioni impartite possono riguardare anche i soggetti autorizzati che non rispettino o non adottino le misure necessarie.

Pierpaolo Pinna – Dirigente Scolastico