



MINISTERO DELL' ISTRUZIONE E DEL MERITO
ISTITUTO COMPRENSIVO BONO

Via Tirso, 07011 Bono Tel. 079 790110- 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

Agli assistenti amministrativi e al
Direttore SGA

Oggetto: Protezione dei dati personali – Regolamento UE 2016/679. Designazione in qualità di soggetti “autorizzati al trattamento di dati personali” dei componenti dell’unità organizzativa “Assistenti Amministrativi e DSGA”.

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. 10 agosto 2018, n. 101 (nel seguito indicato sinteticamente come Codice), ed in particolare l’art. 2-quaterdecies (Attribuzione di funzioni e compiti a soggetti designati), nonché gli artt. 2-sexies e 2-octies in materia di trattamento di categorie particolari di dati e di dati relativi a condanne penali e reati;

VISTO il Codice dell’Amministrazione Digitale (D.Lgs. 7 marzo 2005, n. 82), 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 medesimo e che a questo conferisca, volontariamente o per obbligo, propri dati personali;

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

CONSIDERATO che gli assistenti amministrativi in servizio presso l’Istituto scolastico trattano dati personali in qualità di addetti all’Ufficio di Segreteria, fermi restando gli obblighi e le responsabilità civili e penali;

CONSIDERATO che il DSGA tratta dati personali in qualità del profilo ricoperto all’interno dell’Ufficio di Segreteria, fermi restando gli obblighi e le responsabilità civili e penali;

DETERMINA

1. Di designare l’unità organizzativa **ASSISTENTI AMMINISTRATIVI e Direttore SGA** cui appartengono tutti i dipendenti aventi il profilo di Assistente Amministrativo e il DSGA, quale unità organizzativa **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 entra a far parte di questa unità organizzativa assume automaticamente la funzione di soggetto autorizzato al trattamento e che, in un determinato momento, l’elenco dei soggetti autorizzati

appartenenti a questa unità corrisponde all'elenco dei dipendenti validamente in servizio che ne fanno parte.

3. Di autorizzare i componenti di questa unità organizzativa a trattare tutti 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 dell'intera 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 del trattamento), selezione ed estrazione di dati, connesse alle seguenti funzioni e attività:

Alunni e genitori/tutori

- gestione archivi elettronici alunni e genitori;
- gestione archivi cartacei con fascicoli personali alunni;
- consultazione di documenti e registri di attestazione dei voti e di documentazione della vita scolastica dello studente, nonché delle relazioni tra scuola e famiglia (quali richieste, istanze e corrispondenza con le famiglie);
- gestione di contributi e/o tasse scolastiche versati da alunni e genitori;
- adempimenti connessi alla comunicazione telematica degli infortuni all'INAIL;
- adempimenti connessi ai viaggi e alle uscite di istruzione;

Personale ATA e Docenti

- gestione archivi elettronici del Personale ATA e Docenti;
- gestione archivi cartacei del Personale ATA e Docenti;
- tenuta di documenti e registri relativi alla vita lavorativa dei dipendenti (quali assenze, convocazioni, comunicazioni, documentazione sullo stato del personale, atti di nomina dei supplenti, decreti del Dirigente);

Contabilità e finanza

- gestione archivi elettronici della contabilità;
- gestione di stipendi e pagamenti, nonché adempimenti di carattere previdenziale;
- gestione della documentazione delle ore di servizio (quali la registrazione delle ore eccedenti);
- gestione dei rapporti con i fornitori;
- gestione del Programma annuale e del fondo di istituto;
- corretta tenuta dei registri contabili previsti dal Decreto Interministeriale 28 agosto 2018, n. 129 (Regolamento di contabilità delle istituzioni scolastiche) e dalla correlata normativa vigente.

Protocollo e archivio della corrispondenza ordinaria

- attività di protocollo e archiviazione della corrispondenza ordinaria;

Attività degli organi collegiali

- eventuali operazioni di consultazione ed estrazione di dati dai verbali degli organi collegiali.

L'appartenenza all'unità organizzativa ASSISTENTI AMMINISTRATIVI e DSGA 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. Ad esempio, un assistente amministrativo assegnato all'ufficio alunni potrà accedere ai dati dell'ufficio personale solo previa disposizione ricevuta, anche per sostituire temporaneamente un collega.

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** (trattamento per motivi di interesse pubblico rilevante) e deve avvenire nel rispetto delle tipologie di dati e di operazioni individuate dal Regolamento ministeriale 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 / Disposizioni generali / Atti generali, raggiungibile al seguente link:

https://www.trasparenzascuole.it/Public/AmministrazioneTrasparenteV3.aspx?Customer_id=93f38237-84d6-4e22-91b7-39bd7815efc1&PID=897ce888-55cc-429a-8a8c-4055387b1ee7

6. Fermi restando gli obblighi e le responsabilità civili e penali dei dipendenti pubblici nell'ambito delle attività d'ufficio, 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 AMMINISTRATIVI e DSGA 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;
2. costituisce trattamento qualunque operazione, svolta con o senza l'ausilio di mezzi elettronici o comunque automatizzati, concernente la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione dei dati;
3. il trattamento dei dati personali deve avvenire secondo correttezza e liceità, nel rispetto del D.Lgs. 196/2003 e del Regolamento UE 2016/679;
4. i dati personali oggetto dei trattamenti devono essere esatti e aggiornati e devono inoltre essere pertinenti, completi e non eccedenti rispetto alle finalità per le quali vengono raccolti e trattati;
5. è vietata qualsiasi forma di diffusione e comunicazione dei dati personali trattati che non sia strettamente funzionale allo svolgimento dei compiti affidati e comunque autorizzata dal titolare del trattamento. Si raccomanda particolare attenzione alla tutela del diritto alla riservatezza degli interessati; l'obbligo di riservatezza permane anche oltre il limite temporale dell'incarico;
6. gli atti e i documenti che contengono dati personali non devono mai essere lasciati incustoditi e devono essere adottate misure affinché terzi non autorizzati non possano, anche accidentalmente, accedervi, anche durante il trattamento o in caso di allontanamento temporaneo del soggetto autorizzato;
7. è fatto obbligo di custodire con cura le credenziali di autenticazione attribuite. Le credenziali sono personali e non possono essere rivelate a terzi. In caso di smarrimento o furto è fatto obbligo di darne comunicazione immediata al titolare del trattamento;
8. gli eventuali supporti rimovibili nei quali siano memorizzati dati personali devono essere attentamente custoditi allo scopo di prevenire accessi non autorizzati;
9. 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;
10. al termine del trattamento i documenti contenenti dati personali devono essere riposti e custoditi in contenitori muniti di serratura; la chiave deve essere adeguatamente custodita;
11. i documenti e i registri della scuola contenenti dati personali non possono essere portati all'esterno della sede scolastica né se ne può fare copia se non dietro espressa autorizzazione del titolare del trattamento;
12. le comunicazioni agli interessati dovranno avvenire in forma riservata; se effettuate in forma cartacea dovranno essere consegnate in busta chiusa;

13. *i documenti contenenti dati personali dovranno essere consegnati all'interessato previo accertamento della sua identità o, in caso di delega, previa verifica dell'identità del delegato (la delega deve avere forma scritta);*
14. *nell'ambito dei trattamenti istituzionali, in caso di invio di messaggi di posta elettronica o comunque di comunicazioni in forma elettronica, occorre seguire procedure che garantiscano la riservatezza delle comunicazioni e dei dati trasmessi, richiamati o citati (in particolare, nelle comunicazioni a più destinatari, utilizzare il campo CCN quando è necessario mantenere riservati gli indirizzi di posta elettronica dei destinatari);*
15. **Segnalazione delle violazioni dei dati (data breach).** *Qualunque violazione dei dati personali – perdita, sottrazione, accesso non autorizzato, distruzione o divulgazione accidentale o illecita di dati – o anche il semplice sospetto di essa deve essere segnalata senza ritardo al Dirigente Scolastico e, per il suo tramite, al Responsabile della Protezione dei Dati, al fine di consentire le valutazioni e gli adempimenti previsti dagli artt. 33 e 34 del Regolamento (eventuale notifica al Garante entro 72 ore e comunicazione agli interessati);*
16. **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;*

Il titolare del trattamento precisa che tutte le presenti istruzioni sono vincolanti e obbligatorie e che qualunque violazione delle modalità sopra indicate può dare luogo a specifici provvedimenti disciplinari, oltre a precise responsabilità, ai sensi delle norme contenute nel D.Lgs. 196/2003 e nel Regolamento UE 2016/679.

L'autorizzazione al trattamento dei dati personali 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 Scolastico
(Titolare del trattamento)

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, ai sensi del Regolamento UE 2016/679 e del D.Lgs. 196/2003 (come novellato dal D.Lgs. 101/2018). Ulteriori informazioni sulle modalità del trattamento e sulle misure di sicurezza adottate sono contenute nel registro dei trattamenti. Le presenti indicazioni sono coerenti con le "Misure minime di sicurezza ICT per le pubbliche amministrazioni" adottate da AgID.

1. Regole generali di comportamento

- 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 autorizzati nell'apposito armadio assegnato, accertandosi della corretta funzionalità dei meccanismi di chiusura e segnalando tempestivamente eventuali anomalie;*
- rendere disponibile all'interessato l'informativa predisposta dal titolare del trattamento (artt. 13 e 14 del Regolamento); si ricorda che l'informativa è un adempimento del titolare e non va redatta caso per caso dall'operatore;*
- i trattamenti connessi alle finalità istituzionali della scuola si fondano sull'esecuzione di compiti di interesse pubblico (art. 6, par. 1, lett. e, e art. 9, par. 2, lett. g, del Regolamento; artt. 2-sexies e 2-octies del Codice) e non sul consenso degli interessati; il modulo di consenso va quindi raccolto esclusivamente nei casi residuali in cui il consenso costituisce l'effettiva base giuridica (ad esempio taluni servizi facoltativi o la diffusione di immagini), secondo le indicazioni fornite dal titolare;*
- procedere alla raccolta dei dati con la massima cura, verificandone l'esattezza;*
- accedere ai soli dati personali la cui conoscenza sia strettamente necessaria per lo svolgimento delle funzioni e dei compiti affidati e per le finalità dell'incarico ricevuto;*
- conservare i documenti e gli atti che contengono categorie particolari di dati o dati relativi a condanne penali e reati in archivi (stanze, armadi, schedari, contenitori) chiusi a chiave;*
- non fornire telefonicamente o con altri mezzi dati e informazioni relativi a terzi senza una specifica autorizzazione del titolare;*
- qualora giungano richieste telefoniche di categorie particolari di dati da parte dell'Autorità Giudiziaria o degli organi di polizia, richiedere l'identità del chiamante e provvedere quindi a richiamare, avendo così certezza sull'identità del richiedente;*
- non fornire, anche telefonicamente o per posta elettronica, dati e informazioni ai diretti interessati senza avere la certezza della loro identità;*
- nella comunicazione di categorie particolari di dati adottare sempre procedure che garantiscano la sicurezza e la riservatezza delle informazioni, anche mediante tecniche di anonimizzazione e pseudonimizzazione;*
- distruggere o rendere comunque illeggibili i documenti cartacei non più utilizzati, specie se contenenti categorie particolari di dati, prima di eliminarli;*
- non consentire l'accesso di estranei e di soggetti non autorizzati alle aree in cui sono conservati dati personali su supporto cartaceo o informatico;*
- conservare i documenti ricevuti da genitori, studenti o personale in apposite cartelline non trasparenti e consegnare la documentazione in buste non trasparenti;*

- *effettuare esclusivamente copie (fotostatiche o su supporto informatico) dei documenti per i quali si è autorizzati e non lasciare a disposizione di estranei fotocopie inutilizzate o incomplete, accertandosi che vengano sempre distrutte;*
- *non lasciare incustodito il registro contenente indirizzi e recapiti del personale e degli studenti e non annotarne il contenuto sui fogli di lavoro;*
- *non abbandonare la postazione di lavoro senza aver provveduto a custodire in luogo sicuro i documenti trattati, e 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.*

2. Trattamento di categorie particolari di dati e di dati relativi a condanne penali e reati

Gli assistenti amministrativi, nello svolgimento delle proprie funzioni, possono venire a conoscenza di dati appartenenti a categorie particolari ai sensi dell'art. 9 del Regolamento (UE) 2016/679 e di dati relativi a condanne penali e reati ai sensi dell'art. 10, quali:

- *dati relativi alla salute degli alunni o del personale (certificati medici, documentazione su disabilità, DSA, BES, allergie o intolleranze alimentari, infortuni);*
- *dati che rivelano convinzioni religiose o filosofiche (ad esempio per esoneri da determinate attività o per richieste particolari delle famiglie);*
- *dati che rivelano opinioni sindacali o altre informazioni tutelate dalla normativa.*

Il trattamento di tali dati:

- *è consentito solo nei limiti strettamente indispensabili allo svolgimento dei compiti istituzionali e trova la propria base di liceità negli artt. 2-sexies e 2-octies del Codice (motivi di interesse pubblico rilevante);*
- *deve avvenire secondo il principio di minimizzazione, evitando raccolte superflue o eccedenti rispetto alla finalità;*
- *richiede l'adozione di particolari cautele di custodia (armadi chiusi a chiave, archivi informatici protetti da credenziali personali);*
- *non può comportare la diffusione dei dati né la comunicazione a terzi non autorizzati;*
- *deve avvenire esclusivamente nell'ambito delle procedure autorizzate dall'Istituto, sotto la responsabilità del Dirigente scolastico.*

È fatto assoluto divieto di condividere categorie particolari di dati attraverso canali informali (chat, posta elettronica personale, social network). Eventuali comunicazioni a soggetti esterni (ASL, enti locali, Autorità Giudiziaria) devono sempre essere autorizzate dal Dirigente scolastico e avvenire con canali sicuri.

3. Utilizzo di strumenti di intelligenza artificiale

Nell'utilizzo di strumenti basati sull'intelligenza artificiale per attività amministrative (redazione, riformulazione o sintesi di documenti) il personale autorizzato deve attenersi alle seguenti indicazioni:

- *è vietato inserire dati personali – a maggior ragione se relativi a categorie particolari o a minori – nei prompt forniti a strumenti generalisti non contrattualizzati dalla scuola, poiché ciò può configurare una comunicazione o diffusione di dati priva di base giuridica e priva delle garanzie richieste dal Regolamento;*
- *possono essere utilizzati esclusivamente gli strumenti individuati e autorizzati dall'Istituto, eventualmente nominati responsabili del trattamento;*

- *il testo prodotto dall'IA deve sempre essere riletto e validato da un operatore, sia per verificarne la correttezza sostanziale, sia per accertare che non contenga dati eccedenti rispetto alle finalità della comunicazione.*

4. Trattamenti eseguiti con strumenti informatici

- *utilizzare, per l'accesso ai sistemi informatici, esclusivamente le credenziali di accesso ricevute;*
- *adottare le necessarie cautele per assicurare la segretezza delle credenziali e la diligente custodia di ogni altro dispositivo di autenticazione (badge, schede, chiavi di sicurezza, ecc.); è fatto divieto di comunicare ad altri le proprie credenziali di accesso;*
- *utilizzare, ove disponibile, l'autenticazione a più fattori (MFA) messa a disposizione dall'Istituto;*
- *ogni volta che si abbandoni la postazione di lavoro, porre i PC e i terminali in condizione di non essere utilizzati da estranei, chiudendo le applicazioni in uso e attivando il blocco del sistema mediante password; spegnere sempre il PC alla fine della giornata lavorativa o in caso di assenze prolungate;*
- *in caso di difformità dei dati trattati o di malfunzionamento degli elaboratori, darne immediata comunicazione al titolare del trattamento e all'amministratore di sistema;*
- *mantenere attive e aggiornate le soluzioni di protezione (endpoint) fornite dall'Istituto e verificare i file provenienti da fonti esterne secondo le indicazioni dell'amministratore di sistema;*
- *utilizzare esclusivamente le piattaforme individuate dalla scuola come sicure e da questa nominate responsabili del trattamento, in particolare qualora si rendano necessarie attività lavorative a distanza, secondo le modalità organizzative dell'Istituto e la normativa vigente;*
- *verificare sempre la corretta modifica e/o cancellazione di dati su documenti, cartelle o informazioni condivise cui si abbia accesso (double check), al fine di evitare modifiche o cancellazioni indesiderate che possano arrecare danno agli interessati o limitare il lavoro dei colleghi;*
- *nelle comunicazioni via posta elettronica non usare impropriamente il campo CC, che porterebbe indebitamente a conoscenza di tutti i destinatari i relativi indirizzi; utilizzare il campo CCN quando è necessario mantenere riservati gli indirizzi dei destinatari.*

5. Scelta e gestione delle parole chiave

- *usare una parola chiave di almeno dodici caratteri;*
- *non inserire nella parola chiave riferimenti facilmente riconducibili all'utente (nome, cognome, data di nascita, numeri di telefono, propri o dei familiari);*
- *usare una combinazione di caratteri alfabetici e numerici, preferibilmente con almeno un segno di interpunzione o un carattere speciale;*
- *non riutilizzare la stessa parola chiave su servizi diversi;*
- *modificare la parola chiave 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 e le buone pratiche vigenti;*
- *conservare con cura la parola chiave, evitando di trascriverla su fogli posti in vista in prossimità del PC o sulla rubrica dell'ufficio.*

6. Segnalazione delle violazioni dei dati personali (data breach)

Qualunque violazione dei dati personali – perdita, sottrazione, accesso non autorizzato, distruzione o divulgazione accidentale o illecita di dati – o anche il semplice sospetto di essa, deve essere segnalata senza ritardo al Dirigente Scolastico e, per il suo tramite, al Responsabile della Protezione dei Dati (DPO), al fine di consentire le valutazioni e gli adempimenti previsti dagli artt. 33 e 34 del Regolamento (eventuale notifica al

Garante entro 72 ore e comunicazione agli interessati). La tempestività della segnalazione è essenziale per il rispetto dei termini di legge.

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 dal titolare e/o dai responsabili possono riguardare anche i soggetti autorizzati che non rispettino o non adottino le misure necessarie.

Pierpaolo Pinna – Dirigente scolastico