ISTITUTO COMPRENSIVO "ANGIULLI – DE BELLIS"

Via Carlo Poerio, 31 – 70013 CASTELLANA GROTTE (BA)
Tel. 0804968198 - Cod. Min. BAIC82700Q - Cod. Fisc. 93423110720
e-mail: baic82700q@istruzione.it PEC: baic82700q@pec.istruzione.it Sito internet: www.icangiullidebellis.edu.it

Codice Univoco Ufficio: UFB12V

Circolare n…

Castellana Grotte, 23 aprile 2021

Al DSGA
Agli Assistenti Amministrativi
dell'IC "Angiulli-De Bellis"
Castellana Grotte (BA)

Al sito web

OGGETTO: **protezione dei dati personali ex D.Lgs. n. 196/2003 e Regolamento UE 2016/679 -designazione ad incaricati del trattamenti di dati personali i componenti dell'unità organizzativa "ASSISTENTI AMMINISTRATIVI e DSGA"**

Si invita a prendere visione della circolare in oggetto.

Il Dirigente Scolastico
Gerardo Magro

ISTITUTO COMPRENSIVO "ANGIULLI – DE BELLIS"
Via Carlo Poerio, 31 – 70013 CASTELLANA GROTTE (BA) Tel. 0804968198 - Cod. Min. BAIC82700Q - Cod. Fisc. 93423110720
e-mail: baic82700q@istruzione.it PEC: baic82700q@pec.istruzione.it Sito internet: www.icangiullidebellis.edu.it

Codice Univoco Ufficio: UFB12V

Prot. n.0004083/VII.6 **Castellana Grotte, 23 aprile 2021**

Agli assistenti amministrativi e al DSGA

Oggetto: protezione dei dati personali ex D.lgs. n. 196/2003 e Regolamento UE 2016/679 - designazione ad incaricati del trattamento di dati personali i componenti dell'unità organizzativa "ASSISTENTI AMMINISTRATIVI e DSGA"

IL DIRIGENTE SCOLASTICO

1. **VISTO** il Regolamento UE 2016/679 con particolare riguardo agli artt. 24, 28, 29 e 32;
2. **VISTO** il Decreto Legislativo 30 giugno 2003, n. 196, *"Codice in materia di protezione dei dati personali",* così come modificato dal Decreto Legislativo 10 agosto 2018, n. 101;
3. **CONSIDERATO** che questo Istituto è titolare del trattamento dei dati personali di alunni, genitori, personale dipendente, fornitori, e qualunque altro soggetto che abbia rapporti con l'Istituto medesimo e che a questo conferisca, volontariamente o per obbligo, propri dati personali;
4. **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;
5. **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;
6. **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 DSGA** cui appartengono tutti i dipendenti aventi il profilo di Assistenti Amministrativi e il DSGA quale **incaricata** del trattamento.
2. Di dare atto che ogni dipendente che cessa di far parte di questa unità organizzativa cessa automaticamente dalla funzione di Incaricato, che ogni nuovo dipendente che entra a far parte di questa unità organizzativa assume automaticamente la funzione di Incaricato, che in un determinato momento l'elenco degli incaricati appartenenti a questa categoria corrisponde all'elenco dei dipendenti validamente in servizio che ne fanno parte.
3. Di autorizzare questa categoria di Incaricati 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, in archivi cartacei anche frammentari, nelle memorie dei computers, negli archivi dell'intera scuola e dei dati personali raccolti per l'assolvimento delle finalità istituzionali.
4. Di autorizzare l'unita organizzativa alle operazioni di raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, modifica, comunicazione (nei soli casi autorizzati dal

titolare del trattamento), selezione, estrazione di dati, connesse alle seguenti funzioni e attività esercitate:

Alunni e genitori e tutori responsabili delle strutture di accoglienza

- gestione archivi elettronici alunni e genitori;
- gestione archivi cartacei con fascicoli personali alunni;
- consultazione documenti e registri di attestazione dei voti e di documentazione della vita scolastica dello studente, nonché delle relazioni tra scuola e famiglia quali ad esempio richieste, istanze e corrispondenza con le famiglie;
- gestione contributi e/o tasse scolastiche versati da alunni e genitori;
- adempimenti connessi alla corretta gestione del Registro infortuni;
- adempimenti connessi alle gite scolastiche;

Personale ATA e Docenti

- gestione archivi elettronici Personale ATA e Docenti;
- gestione archivi cartacei Personale ATA e Docenti;
- tenuta documenti e registri relativi alla vita lavorativa dei dipendenti (quali ad es. 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 stipendi e pagamenti, nonché adempimenti di carattere previdenziale;
- gestione documentazione ore di servizio (quali ad esempio, registrazione delle ore eccedenti);
- gestione rapporti con i fornitori;
- gestione Programma annuale e fondo di istituto
- corretta tenuta dei registri contabili

Protocollo e archivio corrispondenza ordinaria

- attività di protocollo e archiviazione della corrispondenza ordinaria;

Attività organi collegiali

- eventuale operazione di consultazione e estrazione dati dai verbali degli organi collegiali.

L'accesso ai dati personali sopra citati da parte del singolo incaricato è consentito solo per lo svolgimento di una specifica mansione od incarico ricevuto in assenza del quale l'appartenenza all'unità organizzativa ASSISTENTI AMMINISTRATIVI non autorizza all'accesso ai dati personali.

5. Di autorizzare l'unità organizzativa a trattare i dati sensibili e giudiziari con cui vengano a contatto durante l'attività di loro competenza nei limiti previsti dal ***regolamento per il trattamento dei dati sensibili e giudiziari*** secondo quanto previsto dal D.M 305/2006, pubblicato sulla G.U. n°11 del 15-01-07; L'appartenenza alla unità organizzativa ASSISTENTI AMMINISTRATIVI non autorizza all'accesso indiscriminato ai dati personali e sensibili trattati dall'amministrazione che dovrà invece essere autorizzato per ogni singolo incaricato in base alle mansioni da svolgere e all'incarico ricevuto.
6. Fermi restando obblighi e responsabilità civili e penali dei dipendenti pubblici nell'ambito delle attività d'ufficio, di disporre sotto vincolo disciplinare l'obbligo tassativo di attenersi alle suddette istruzioni per tutti i dipendenti facenti parte 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 seguendo le prescrizioni di cui al D.lgs. 196/2003 e Regolamento UE 679/2016.
4. I dati personali, oggetto dei trattamenti, devono essere esatti ed aggiornati, inoltre devono essere pertinenti, completi e non eccedenti le 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; non comunicare a terzi, al di fuori dell'ambito lavorativo, o in difformità dalle istruzioni ricevute, qualsivoglia dato personale; l'obbligo di riservatezza permane anche oltre il limite temporale dell'incarico.
6. Gli atti e i documenti che contengono dati personali non devono essere mai lasciati incustoditi e devono essere adottate misure affinché terzi non autorizzati possano anche accidentalmente accedervi, anche durante il trattamento o in caso di allontanamento temporaneo dell'incaricato.
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 dei dati.
8. Eventuali supporti rimovibili nei quali siano memorizzati dati personali devono essere attentamente custoditi allo scopo di prevenire accessi non autorizzati.
9. L'accesso a dati sensibili o giudiziari è permesso solo alle persone autorizzate e 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. Documenti, 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 per scritto dovranno essere consegnate in busta chiusa.
13. I documenti contenenti dati personali dovranno essere consegnati all'interessato previo accertamento dell'identità dello stesso o -in caso di delega- previa verifica dell'identità del delegato (la delega deve avere forma scritta).
14. Nell'ambito dei trattamenti istituzionali, nel caso di invio di mail o comunque di comunicazioni in forma elettronica occorre seguire procedure che garantiscano la riservatezza delle comunicazioni e dei dati trasmessi o richiamati o citati.

Qualunque violazione delle modalità sopra indicate e delle linee guida consegnate con la presente dà luogo a precise responsabilità ai sensi delle norme contenute nel D L.vo 196/03 e nel Regolamento UE 2016/679.

IL DIRIGENTE SCOLASTICO
Dott. Gerardo MAGRO

ISTITUTO COMPRENSIVO "ANGIULLI – DE BELLIS"
Via Carlo Poerio, 31 – 70013 CASTELLANA GROTTE (BA) Tel. 0804968198 - Cod. Min. BAIC82700Q - Cod. Fisc. 93423110720
e-mail: baic82700q@istruzione.it PEC: baic82700q@pec.istruzione.it Sito internet: www.icangiullidebellis.edu.it

Codice Univoco Ufficio: UFB12V

Prot.n. ***Prot. n.0004083/VII.6*** *Castellana Grotte, 23 aprile 2021*

LINEE GUIDA IN MATERIA DI SICUREZZA PER IL PERSONALE AMMINISTRATIVO INCARICATO DEL TRATTAMENTO

Vengono di seguito riportate le norme cui dovrà attenersi il personale amministrativo incaricato del 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 rappresenti;
- 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 cifratura, 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;
- 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 dì 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.)
- E' fatto divieto 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
- spegnere 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.

Per l'attività lavorativa svolta da remoto dovranno essere osservate le disposizioni contenute nel regolamento per le attività in smart working.

Regole per la scelta delle parole chiave

- usare una parola chiave di almeno otto 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 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
Dott. Gerardo Magro

ISTITUTO COMPRENSIVO "ANGIULLI – DE BELLIS"
Via Carlo Poerio, 31 – 70013 CASTELLANA GROTTE (BA)
Tel. 0804968198 - Cod. Min. BAIC82700Q - Cod. Fisc. 93423110720
e-mail: baic82700q@istruzione.it PEC: baic82700q@pec.istruzione.it Sito internet: www.icangiullidebellis.edu.it
Codice Univoco Ufficio: UFB12V

Norme di comportamento del dipendente nelle attività lavorative svolte nella modalità di lavoro agile

Portiamo a conoscenza del personale che svolge la propria attività in modalità di lavoro agile le raccomandazioni elaborate da Cert-PA di AgID per il rispetto delle misure minime di sicurezza informatica per le pubbliche amministrazioni fissate dalla circolare 17 marzo 2017, n. 1 che devono essere garantite anche dal personale che svolge la propria attività lavorativa da remoto:

1. Segui prioritariamente le policy e le raccomandazioni dettate dalla tua Amministrazione
2. Utilizza i sistemi operativi per i quali attualmente è garantito il supporto (non utilizzare, ad esempio, macchine con sistema operativo windows XP o windows 7 di cui microsoft ha terminato il supporto)
3. Effettua costantemente gli aggiornamenti di sicurezza del tuo sistema operativo
4. Assicurati che i software di protezione del tuo sistema operativo (Firewall, Antivirus, ecc) siano abilitati e costantemente aggiornati
5. Assicurati che gli accessi al sistema operativo siano protetti da una password sicura di almeno 8 caratteri contenente almeno una lettera maiuscola, un numero ed un carattere speciale
6. Non installare software proveniente da fonti/repository non ufficiali
7. Blocca l'accesso al sistema e/o configura la modalità di blocco automatico quando ti allontani dalla postazione di lavoro
8. Non cliccare su link o allegati contenuti in email sospette
9. Utilizza l'accesso a connessioni Wi-Fi adeguatamente protette
10. Collegati a dispositivi mobili (pen-drive, hdd-esterno, etc) di cui conosci la provenienza (nuovi, già utilizzati, forniti dalla tua Amministrazione)
11. Effettua sempre il log-out dai servizi/portali utilizzati dopo che hai concluso la tua sessione lavorativa.

Si coglie l'occasione per dare le seguenti ulteriori disposizioni:

- Nel caso in cui utilizzi un PC personale per svolgere l'attività lavorativa, prima del suo primo utilizzo, installa un buon antivirus e fai una accurata scansione preventiva per rimuovere qualunque software malevolo
- Non memorizzare sui dispositivi le password di accesso alle piattaforme ed ai sistemi utilizzati per il lavoro a distanza
- Non memorizzare sul client di posta elettronica le credenziali di accesso alle caselle istituzionali
- Accertati di aver impostato una password sicura sul router utilizzato per l'accesso ad Internet (accertati di non aver lasciato la password di default proposta dal costruttore e nota a qualunque malintenzionato)
- Se utilizzi una connessione wifi, accertati di adottare una password sicura per il suo accesso (mai lasciare accessi liberi alla rete wifi)