



ISTITUTO COMPRENSIVO DI BUJA

per le scuole dell'Infanzia e Primarie dei Comuni di Buja e Treppo Grande e
per la Scuola Secondaria di 1° grado del Comune di BUJA - CODICE UNIVOCO UF2F3C

Via Brigata Rosselli, 6 - 33030 BUJA (Ud) - Tel. 0432/960232 - Fax 0432/961714 - cod. fisc. 82000500304

Sito internet www.icbuja.edu.it e-mail UDIC82800X@istruzione.it UDIC82800X@pec.istruzione.it



LINEE GUIDA per una corretta gestione della privacy e della sicurezza nei luoghi di lavoro

Normativa di riferimento:

Regolamento Europeo 2016/679

D.lgs. n.101/2018

Circolare AgID 18 aprile 2017 n.2 ("Misure minime di sicurezza ICT per le Pubbliche Amministrazioni")

PERSONALE D.S.G.A e ASSISTENTI AMMINISTRATIVI

1. Non comunicare a nessun soggetto non specificatamente autorizzato i dati personali comuni, sensibili, giudiziari, sanitari e/o altri dati, elementi, informazioni dei quali il personale viene a conoscenza nell'esercizio delle Sue funzioni. In caso di dubbio accertarsi sempre dal Titolare del trattamento se il soggetto cui devono essere comunicati i dati sia o meno autorizzato a riceverli.
2. Prestare particolare attenzione ai dati importanti di cui si è personalmente responsabili e, laddove sia difficile distinguerli, è buona norma trattare tutti i dati come importanti.
3. Maneggiare e custodire con cura circolari, comunicazioni, lettere ed altro materiale riservato.
4. Vigilare i locali della Segreteria affinché soggetti terzi, estranei alla scuola e, quindi, al trattamento dei dati, non possano entrare in contatto con le informazioni in possesso della scuola nè vengano in possesso di circolari, comunicazioni, lettere ed altro materiale riservato e consegnato al personale.
5. Chiudere i documenti a chiave nei cassetti o negli armadi alla fine della giornata e ogni volta possibile. Al fine di evitare promiscuità di dati personali.
6. Chiudere l'Ufficio in caso di allontanamento o in caso di assenza di personale al suo interno.
7. Verificare la corretta funzionalità della chiusura degli armadi che custodiscono dati personali, segnalando tempestivamente al DSGA eventuali anomalie.
8. Conservare supporti di memoria e stampe in luoghi sicuri ricordando che agli stessi (CD, chiavette USB, hard disk esterni) si applicano gli stessi criteri di protezione dei documenti cartacei.
9. Non lasciare documenti (circolari, comunicazioni, lettere, fascicoli, appunti...) sulla scrivania se il personale si allontana dalla postazione di lavoro (pausa o altro motivo). Sono da evitare situazioni di promiscuità dei dati personali.
10. Fare fotocopie di documenti contenenti dati personali sensibili solo se strettamente necessario. Non lasciare copie nella stampante/fotocopiatrice e, se necessario, eliminare copie mal riuscite con una macchina distruggi-documenti (shredder) o strapparli manualmente.
11. Accertarsi che non accedano alle stampe persone non autorizzate. Se la stampante non si trova sulla scrivania recarsi quanto prima a ritirare il documento.
12. Utilizzare hardware e software in modo conforme ed esclusivamente per lo svolgimento delle attività professionali cui ogni incaricato è preposto.
13. E' fatto divieto di
 - salvare la password e i codici di accesso personali all'interno del computer della scuola;
 - navigare in siti non attinenti l'attività lavorativa;
 - partecipare a forum, mailing list, chat o altro non attinente l'attività lavorativa;
 - scaricare per qualsiasi finalità, anche connesse con l'attività lavorativa, programmi reperiti in rete (internet) o da qualunque altra sorgente esterna salvo espressa autorizzazione del Titolare. Costituiscono illecito penale le condotte consistenti nell'illecita duplicazione o riproduzione di software ai sensi della legge sul diritto d'autore n. 633/41 e s.m..
14. Assicurare le stesse procedure di tutela del trattamento, conservazione, integrità dei dati personali anche in caso di utilizzo di dispositivi informatici personali;
15. Controllate se nella barra degli indirizzi del browser di navigazione (Google Chrome, Mozilla Firefox, Microsoft Edge) il protocollo di navigazione è *http* oppure *https* (oppure se compare

l'icona di un lucchetto). La presenza dell'icona e/o della scritta https assicura che i dati oggetto di trasmissione sono cifrati e quindi non intelligibili.

16. Non comunicate alla stampa giornalistica e/o televisiva notizie, fatti, informazioni di cui a conoscenza nello svolgimento dell'attività lavorativa.

Per ogni ulteriore informazione si invita a contattare il Dirigente Scolastico e il D.S.G.A..

PERSONALE COLLABORATORE SCOLASTICO

1. Non comunicare a nessun soggetto non specificatamente autorizzato i dati personali comuni, sensibili, giudiziari, sanitari e/o altri dati, elementi, informazioni dei quali il personale viene a conoscenza nell'esercizio delle Sue funzioni. In caso di dubbio accertarsi sempre dal Titolare del trattamento se il soggetto cui devono essere comunicati i dati sia o meno autorizzato a riceverli.
2. Prestare particolare attenzione ai dati importanti di cui si è personalmente responsabili e, laddove sia difficile distinguerli, è buona norma trattare tutti i dati come importanti.
3. Maneggiare e custodire con cura circolari, comunicazioni, lettere ed altro materiale riservato non lasciando che terzi accedano o vengano in possesso di circolari, comunicazioni, lettere ed altro materiale riservato consegnato al personale.
4. Controllare che i documenti siano posizionati in luoghi sicuri e che le aule/uffici restino chiusi in assenza di personale al loro interno.
5. Non lasciare documenti (circolari, comunicazioni, lettere, fascicoli, appunti...) sul tavolo di lavoro se il personale si allontana dalla postazione (pausa o altro motivo). Sono da evitare situazioni di promiscuità dei dati personali.
6. Durante lo svolgimento delle proprie mansioni accertarsi che, al termine delle lezioni, non restino incustoditi, nelle aule o in altri spazi, documenti contenenti dati personali o sensibili degli alunni o dei docenti. L'eventuale presenza deve essere tempestivamente segnalata al referente di sede/plesso provvedendo temporaneamente alla loro custodia.
7. Conservare supporti di memoria e stampe in luoghi sicuri ricordando che agli stessi (CD, chiavette USB, hard disk esterni) si applicano gli stessi criteri di protezione dei documenti cartacei.
8. Fare fotocopie di documenti contenenti dati personali sensibili solo se strettamente necessario. Non lasciare copie nella stampante/fotocopiatrice e, se necessario, eliminare copie mal riuscite con una macchina distruggi-documenti (shredder) o strapparli manualmente.
9. Utilizzare hardware e software in modo conforme ed esclusivamente per lo svolgimento delle attività professionali cui ogni incaricato è preposto.
10. Controllate se nella barra degli indirizzi del browser di navigazione (Google Chrome, Mozilla Firefox, Microsoft Edge) il protocollo di navigazione è *http* oppure *https* (oppure se compare l'icona di un lucchetto). La presenza dell'icona e/o della scritta *https* assicura che i dati oggetto di trasmissione sono cifrati e quindi non intelligibili.
11. Durante lo svolgimento delle proprie mansioni accertarsi che, al termine delle lezioni, i computers dell'aula di informatica siano spenti e che siano stati lasciati incustoditi cd, dvd, chiavette usb o hard disk, cartelle o altri materiali. L'eventuale presenza deve essere tempestivamente segnalata al referente di sede/plesso provvedendo temporaneamente alla loro custodia.
12. Procedere alla chiusura dell'edificio scolastico accertandosi che tutte le misure di protezione dei locali siano state attivate.
13. Non lasciare incustodito il registro contenente gli indirizzi e i recapiti telefonici del personale e delle famiglie degli allievi e non annotarne il contenuto sui fogli di lavoro.
14. Non comunicare alla stampa giornalistica e/o televisiva notizie, fatti, informazioni di cui a conoscenza nello svolgimento dell'attività lavorativa.

Per ogni ulteriore informazione si invita a contattare il Dirigente Scolastico e il D.S.G.A..

PERSONALE DOCENTE

1. Non comunicare a nessun soggetto non specificatamente autorizzato i dati personali comuni, sensibili, giudiziari, sanitari e/o altri dati, elementi, informazioni dei quali il docente viene a conoscenza nell'esercizio delle Sue funzioni. In caso di dubbio accertarsi sempre dal Titolare del trattamento se il soggetto cui devono essere comunicati i dati sia o meno autorizzato a riceverli.
2. Controllare che i documenti siano posizionati in luoghi sicuri e che le aule/uffici restino chiusi in assenza di personale al loro interno.
3. Porre in essere e osservare i seguenti accorgimenti nelle attività di trattamento dei dati (compresa la documentazione contenente dati personali):
 - non far uscire documenti dalla sede scolastica, neanche temporaneamente, salvo ciò non sia assolutamente necessario per l'espletamento dell'incarico e vi sia l'autorizzazione del Dirigente Scolastico;
 - non fare copie della documentazione salvo autorizzazione del Dirigente Scolastico/D.S.G.A.;
 - mantenere i documenti contenenti dati personali lontani dalla vista di terzi estranei;
 - custodire i documenti all'interno di archivi;
 - consegnare immediatamente in Ufficio di Segreteria dati sensibili e giudiziari su cui si viene in possesso;
 - in caso di allontanamento anche temporaneo dal luogo di lavoro, l'incaricato dovrà verificare che non vi sia possibilità da parte di terzi, anche se dipendenti ma non incaricati, di accedere a dati personali per i quali è in corso un qualunque tipo di trattamento.
4. Conservare in apposita busta nel registro di classe e/o agenda i documenti contenenti dati personali o sensibili degli alunni per l'anno scolastico in corso e, alla sua conclusione consegnare la busta all'ufficio di Segreteria.
5. Proteggere attentamente i dati in possesso e di cui si è personalmente responsabile.
6. Posizionare i dati in un'area protetta da password e non dare automaticamente a nessun altro utente il permesso di lettura o modifica. Ai dati da condividere applicare i permessi opportuni solo per il tempo strettamente necessario all'interazione con gli altri utenti.
7. Spegnerne il computer se il docente si assenta per un periodo di tempo lungo. Un computer acceso può essere maggiormente attaccabile perché raggiungibile tramite la rete o direttamente sulla postazione di lavoro.
8. Fare fotocopie di documenti contenenti dati personali sensibili solo se strettamente necessario. Non lasciare copie nella macchina e se necessario eliminare copie mal riuscite utilizzate una macchina distruggi-documenti (shredder) o strappandole manualmente.
9. Non lasciare lavori incompiuti sullo schermo del computer utilizzato. E' bene chiudere sempre le applicazioni con cui si sta lavorando in caso di allontanamento.
10. Eliminare la bozza di lavoro dal computer o in alternativa anonimizzare il documento espungendo il testo dalle informazioni identificative. La stessa regola vale nell'ipotesi in cui il docente utilizzi dispositivi personali.
11. Abilitare l'accesso al computer portatili tramite la password ed effettuare periodicamente il backup dei dati

12. Non permettere l'uso del proprio account ad altri colleghi in quanto un'attività illecita svolta da un collega con la password del docente sarà attribuita al docente stesso, con tutte le conseguenze giuridiche del caso.
13. Non installare programmi non autorizzati al fine di non trasferire involontariamente un virus o introdurre un cosiddetto "cavallo di troia".
14. E' fatto divieto di
 - salvare la password e i codici di accesso personali all'interno del computer della scuola;
 - navigare in siti non attinenti l'attività lavorativa;
 - partecipare a forum, mailing list, chat o altro non attinente l'attività lavorativa;
 - scaricare per qualsiasi finalità, anche connesse con l'attività lavorativa, programmi reperiti in rete (internet) o da qualunque altra sorgente esterna salvo espressa autorizzazione del Titolare. Costituiscono illecito penale le condotte consistenti nell'illecita duplicazione o riproduzione di software ai sensi della legge sul diritto d'autore n. 633/41 e s.m..
15. Utilizzare hardware e software in modo conforme ed esclusivamente per lo svolgimento delle attività professionali cui ogni incaricato è preposto.
16. Controllate se nella barra degli indirizzi del browser di navigazione (Google Chrome, Mozilla Firefox, Microsoft Edge) il protocollo di navigazione è *http* oppure *https* (oppure se compare l'icona di un lucchetto). La presenza dell'icona e/o della scritta *https* assicura che i dati oggetto di trasmissione sono cifrati e quindi non intelligibili.
17. Consultare la documentazione relativa agli allievi diversamente abili/BES presso l'Ufficio di Segreteria. E' fatto divieto di fare fotocopie o scansioni della documentazione stessa.
18. Accertarsi che al termine delle lezioni non restino incustoditi, nelle aule o in altri spazi, i documenti: contenenti dati personali o sensibili degli alunni o dei docenti.
19. Avvisare il Titolare in caso di perdita o distruzione, anche accidentali, di dati personali, e in generale in tutti i casi in cui l'incaricato ragionevolmente ritenga che vi possa essere stata una violazione degli stessi (accessi indebiti, accessi non autorizzati, sottrazione o perdita di password e/o codici di accesso, divulgazione di dati personali non autorizzata, ecc.).
20. Assicurare le stesse procedure di tutela del trattamento, conservazione, integrità dei dati personali anche in caso di utilizzo di dispositivi informatici personali;
21. Segnalare al Dirigente Scolastico o al DSGA eventuali anomalie o guasti nei sistemi di chiusura degli armadi o dei contenitori adibiti ad archivio.
22. Non comunicare alla stampa giornalistica e/o televisiva notizie, fatti, informazioni di cui a conoscenza nello svolgimento dell'attività lavorativa.

Per ogni ulteriore informazione si invita a contattare il Dirigente Scolastico e il D.S.G.A..

GLOSSARIO (art. 4 del GDPR 2016/679)

General Data Protection Regulation

DATO PERSONALE	E' qualsiasi informazione che identifica (o rende identificabile) direttamente o indirettamente una persona fisica (es. nome e cognome, indirizzo; Codice Fiscale, Partita Iva; numeri di telefono/cell; foto; e-mail).
DATO IDENTIFICATIVO	E' il dato che permette l'identificazione diretta dell'interessato.
DATO ANONIMO	E' il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile.
DATO SENSIBILE	<i>Art. 9 "I dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché i dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona".</i> I dati sensibili possono essere trattati solo previo consenso dell'interessato.
DATO RELATIVO A CONDANNE PENALI E REATI	E' il dato personale che può rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale o la qualità di imputato o di indagato. <i>Art.10 "Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'art. 6, co. 1, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati".</i>
DATO RELATIVO ALLA SALUTE	E' il dato personale attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute.
TITOLARE DEL TRATTAMENTO	E' la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali. Il titolare del trattamento è l'Istituto Scolastico rappresentato dal Dirigente Scolastico in carica pro tempore.
RESPONSABILE DEL TRATTAMENTO	E' la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo interno o esterno che tratta dati personali per conto del titolare del trattamento. E' nominato con atto scritto e si attiene alle istruzioni ricevute dal titolare.
INCARICATO DEL TRATTAMENTO	E' la persona fisica o l'unità organizzativa autorizzata o istruita dal titolare o dal responsabile a compiere operazioni di trattamento sui dati personali.
INTERESSATO data subject	E' la persona fisica alla quale si riferiscono i dati trattati. .E' il soggetto "proprietario" dei dati personali e su questi conserva dei diritti nei confronti del titolare del trattamento. Sono considerati interessati : alunni, famiglie, personale tecnico-amministrativo, personale docente, collaboratori scolastici, fornitori , utenti del sito web istituzionale.

DESTINATARIO	<p>Art. 4 E' "<i>la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi</i>".</p> <p>Sono considerati destinatari tutti i soggetti che ricevono dati personali da un titolare, sia che siano interni o esterni, sia che li ricevono per eseguire trattamenti per conto del titolare sia che li ricevono per conseguire proprie finalità.</p>
TRATTAMENTO	<p>Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.</p>
INFORMATIVA	<p>Il titolare, anche attraverso i propri incaricati, deve fornire preventivamente all'interessato le informazioni di cui all'art. 13 del Regolamento circa la natura e le modalità del trattamento posto in essere, utilizzando i modelli predisposti dal titolare.</p>
CONSENSO DELL'INTERESSATO	<p>Qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento. Se il trattamento riguarda dati sensibili o giudiziari, il consenso va espresso per iscritto.</p>
SICUREZZA DELL'INFORMAZIONE	<p>Riservatezza Prevenzione contro l'accesso non autorizzato alle informazioni Integrità le informazioni non devono essere alterabili da violazioni, incidenti o abusi</p>
DIRITTO ALLA RETTIFICA	<p>L'interessato ha la possibilità di richiedere, in qualsiasi momento, la modifica dei propri dati personali qualora questi risultino inesatti.</p>
DIRITTO ALLA CANCELLAZIONE (all'oblio)	<p>L'interessato ha la possibilità di richiedere la totale cancellazione dei propri dati personali presso un determinato titolare del trattamento. Tale diritto può essere esercitato anche dopo la revoca del consenso al trattamento.</p>
DIRITTO DI ACCESSO	<p>L'interessato ha il diritto di richiedere e ottenere, al titolare del trattamento, la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano, con una descrizione esatta delle modalità e finalità. L'accesso al dato può avvenire da remoto oppure chiedere una copia.</p>
DIRITTO DI OPPOSIZIONE	<p>L'interessato ha la possibilità di opporsi, in qualsiasi momento e per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano.</p>