Istituto Comprensivo "SAN GIOVANNI BOSCO"
Via Mazzini n°62 – 94012 Barrafranca (EN)
C.F. 91003950861 – C.M. enic824005
EMAIL: enic824005@istruzione.it - PEC: enic824005@pec.istruzione.it - tel./fax 0934-464274

Com. n°37
Prot. N°3914/A-32

Barrafranca 06/10/2015
Al personale amministrativo
SEDE

Al fine di garantire la normativa sulla privacy nello svolgimento dei propri compiti di ufficio, si trasmettono le seguenti **LINEE GUIDA IN MATERIA DI SICUREZZA PER Gli ASSISTENTI AMMINISTRATIVI INCARICATI DEL TRATTAMENTO DEI DATI.**

Il responsabile del trattamento dei dati, limitatamente all'area amministrativa, è la DSGA, in quanto in possesso dei requisiti al comma 2 dell'art. 29 del D.L.vo 196/2003. I predetti trattamenti riguardano le seguenti tipologie di dati:

a) alunni e genitori:
- dati anagrafici e di percorso scolastico;
- dati sensibili in relazione a condizione di disabilità, assenze per malattia, origine etnica e opzioni religiose;
- dati di contesto famigliare nelle rilevazioni campionarie attuate dall'I.N.VAL.S.I. o altri soggetti autorizzati dal MIUR;
- corrispondenza scuola-famiglie;

b) personale dipendente o contrattualizzato:
- dati anagrafici;
- dati afferenti allo stato giuridico ordinario;
- dati relativi all'affidamento di incarichi aggiuntivi o specifici conferiti;
- dati, anche sensibili, relativi alle cause di assenza dal lavoro;
- dati riferibili alle opzioni sindacali.

c) funzionamento degli OO.CC:
- dati anagrafici e elettorali dei membri;
- dati presenti nelle verbalizzazioni;

d) soggetti esterni:
- dati anagrafici o riferibili allo status giuridico di fornitori o collaboratori esterni;
- dati contenuti in offerte, transazioni economico-commerciali etc.

1) TIPOLOGIE DEI DATI PERSONALI TRATTABILI

a) dati sensibili e giudiziari gestiti nel protocollo riservato riguardanti:
- alunni e genitori/affidatari;
- personale dipendente o contrattualizzato, inclusi quelli relativi a contenzioso, reclami, sanzioni disciplinari etc;
- funzionamento degli OO.CC., con riguardo a sanzioni disciplinari, verbalizzazioni recanti apprezzamenti di carattere personale etc;
- soggetti esterni per reclami, denunce, istanze giudiziarie etc.

b) dati personali presenti nei seguenti atti:
- programma annuale, conto consuntivo e altre scritture contabili; - contratti di acquisto, fornitura o di prestazione d'opera con soggetti esterni;
- documenti relativi ai compensi a favore del personale interno;

c) dati personali presenti negli atti relativi ai passaggi di consegne fra DSGA uscente e subentrante.

E' fatto divieto, in assenza di specifica autorizzazione del D.S.G.A. o del Dirigente scolastico, agli assistenti amministrativi, di trattare dati personali non pertinenti con l'incarico affidato.

2) FINALITA'

Tutti i trattamenti dovranno essere effettuati unicamente per le finalità istituzionali ed in ottemperanza a prescrizioni normative o su richiesta dell'interessato.

3) ACQUISIZIONE

L'acquisizione dei dati dovrà avvenire esclusivamente:
- per fornitura diretta da parte dell'interessato;
- per trasmissione da parte di altre amministrazioni o da altri uffici dell'istituzione scolastica;;
- per passaggio di consegne negli avvicendamenti del personale di segreteria.

4) MODALITA' DI TRATTAMENTO

Tutti i trattamenti sono effettuati mediante elaborazioni su supporto cartaceo o informatico; i predetti supporti dovranno essere custoditi:
- nell'archivio storico;
- nell'archivio corrente;
- sulle memorie dei PC in dotazione agli uffici di segreteria o dei server connessi in rete;
- in cassaforte di sicurezza (dati sensibili, giudiziari e afferenti al protocollo riservato).

L'elaborazione informatica comprende anche le operazioni:
a) gestione delle pass-word;
b) protezione e salvataggio;
c) misure per evitare l'accesso non autorizzato di estranei al PC in dotazione;
d) la correzione di eventuali dati errati;
e) la collocazione e custodia protetta di eventuali memorie esterne (floppy-disc, CD-rom, pen-drive, hard-disk esterni etc).

L'elaborazione cartacea comprende anche:
a) la riunione di parti in fascicoli spillati in modo da evitare la dispersione dei fogli e la conservazione dei documenti in cartelle etichettate e, ove occorre, codificate, in modo da permettere il rapido recupero;
b) la individuazione di spazi delimitati in cui collocare i documenti in modo da consentire il rapido recupero;
c) misure per evitare l'accesso non autorizzato ai documenti presenti nella propria postazione di lavoro;
d) la gestione delle chiavi di accesso ai locali e ai contenitori ove vengono custoditi i documenti;
e) la correzione di eventuali dati errati;

Le informazioni relative alle predette modalità dovranno essere puntualmente comunicate al collega subentrante in occasione di mutamenti di incarichi o mansioni.

5) COMUNICAZIONE E DIFFUSIONE

I dati trattati possono essere comunicati unicamente a:
- altre scuole;
- uffici ministeriali;
- uffici pubblici territoriali o nazionali quali: ASL, uffici dell'Economia e del Lavoro, inps, inpdap, EE.LL. Tribunali etc;
- ove previsto o autorizzato, a OO.SS. di categoria o associazioni professionali.

E' fatto divieto, in assenza di specifica autorizzazione di comunicare dati personali in proprio possesso a terzi non autorizzati.

Indicazioni per garantire la sicurezza dei dati personali e, in particolare, dei dati sensibili e giudiziari :

- Conservare sempre i dati del cui trattamento si è incaricati in apposito armadio assegnato, dotato di serratura;
- Accertarsi della corretta funzionalità dei meccanismi di chiusura dell'armadio, segnalando tempestivamente al Responsabile eventuali anomalie;
- 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 al fax e alla stampante che contengano documenti non ancora ritirati dal personale;
- Effettuare esclusivamente copie fotostatiche di documenti per i quali si è autorizzati;
- Provvedere personalmente alla distruzione quando è necessario eliminare documenti inutilizzati;
- 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 Responsabile o dal Titolare.

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

- Non lasciare floppy disk, cartelle o altri documenti a disposizione di estranei;
- Conservare i dati sensibili in armadi chiusi, ad accesso controllato o in files protetti da password;
- Non consentire l'accesso ai dati a soggetti non autorizzati;
- Riporre i supporti in modo ordinato negli appositi contenitori e chiudere a chiave classificatori e armadi dove sono custoditi;
- Scegliere una password con le seguenti caratteristiche:
  - originale
  - composta da otto caratteri
  - che contenga almeno un numero
  - che non sia facilmente intuibile, evitando il nome proprio, il nome di congiunti, date di nascita e comunque riferimenti alla propria persona o lavoro facilmente ricostruibili
- curare la conservazione della propria password ed evitare di comunicarla ad altri;
- cambiare periodicamente (almeno una volta ogni tre mesi) la propria password;
- modificare prontamente (ove possibile) la password assegnata dal custode delle credenziali;
- trascrivere su un biglietto chiuso in busta sigillata e controfirmata la nuova password e consegnarla al custode delle credenziali;
- spegnere correttamente il computer al termine di ogni sessione di lavoro;
- non abbandonare la propria postazione di lavoro per la pausa o altri motivi senza aver spento la postazione di lavoro o aver inserito uno screen saver con password;
- comunicare tempestivamente al Titolare o al Responsabile qualunque anomalia riscontrata nel funzionamento del computer;
- non riutilizzare i supporti informatici utilizzati per il trattamento di dati sensibili per altri trattamenti;
- non gestire informazioni su più archivi ove non sia strettamente necessario e comunque curarne l'aggiornamento in modo organico;
- utilizzare le seguenti regole per la posta elettronica:
- non aprire documenti di cui non sia certa la provenienza
- non aprire direttamente gli allegati ma salvarli su disco e controllarne il contenuto con un antivirus
- inviare messaggi di posta solo se espressamente autorizzati dal Responsabile
- controllare accuratamente l'indirizzo dei destinatario prima di inviare dati personali.

ISTITUTO COMPRENSIVO "SAN GIOVANNI BOSCO" BARRAFRANCA

IL DIRIGENTE SCOLASTICO
(Dott.ssa Luigia Maria Emilia Perricone)