**ISTITUTO COMPRENSIVO STATALE "BALSAMO- PANDOLFINI"**

***Salita San Girolamo - 90018 Termini Imerese (PA)***

*/fax n° 091/8190251 - C. F.:87000950821 - Cod.Mec.:PAIC88600N*
*e-mail: paic88600n@istruzione.it -*
*paic88600n@pec.istruzione.it*
*sito: www.icsbalsamopandolfini.gov.it*

**Circolare n. 22/2019**

**AI DOCENTI E PERSONALE ATA**
**DELL' ISTITUTO COMPRENSIVO**
**BALSAMO- PANDOLFINI**

Sito area privacy

**Oggetto: Obblighi in materia di privacy**

Premesso che tutti i docenti d'Istituto e il personale ATA sono stati designati, nell'ambito della normativa sulla privacy, come incaricati al trattamento dei dati sia ordinari che sensibili, con la presente si riepilogano le misure da rispettare al fine di garantire la sicurezza e l'integrità dei dati.

In particolare si ricorda il seguente obbligo:

- divieto di comunicazione e diffusione dei dati trattati nel corso dell'incarico e a non utilizzare i dati, cui abbia accesso, per finalità incompatibili con quelle relative al profilo di appartenenza. Si ricorda che le operazioni di comunicazione e diffusione di dati sensibili sono possibili quando vi sia una apposita previsione di legge o di regolamento.

Si confida nella puntuale applicazione delle disposizioni indicate.

Lo presente circolare è pubblicata sul sito dell'istituto nella sezione privacy.

Il
Dirigente Scolastico
Prof. Angelini Fabio

*Il documento è firmato digitalmente ai sensi del D.Lgs. 82/2005 s.m.i. e norme collegate e sostituisce il documento cartaceo e la firma autografa*

Firmato da:
Fabio Angelini
Motivo:
atti

Data: 23/09/2019 09:23:48

**ISTITUTO COMPRENSIVO STATALE "BALSAMO- PANDOLFINI"**

***Salita San Girolamo - 90018 Termini Imerese (PA)***

*/fax n° 091/8190251 - C. F.:87000950821 - Cod.Mec.:PAIC88600N*
*e-mail: paic88600n@istruzione.it -*
*paic88600n@pec.istruzione.it sito:*
*www.icsbalsamopandolfini.gov.it*

Misure da applicare per garantire la sicurezza e l'integrità dei dati a cura degli incaricati al trattamento:

**1) TRATTAMENTO CON L'AUSILIO DI STRUMENTI ELETTRONICI**

**In caso di trattamento di dati personali con l'ausilio di strumenti elettronici:**

 le postazioni di lavoro non devono essere mai lasciate incustodite e devono avere una password di accesso;

 in caso di assenza temporanea l'addetto deve chiudere o spegnere o disattivare la postazione. Nel caso, invece, di assenza prolungata dell'addetto al trattamento dei dati personali e di motivata esigenza di utilizzo dei dati medesimi, il dirigente assicura, con atto formale, che le credenziali di accesso alla postazione siano trasferite ad altro addetto, che è tenuto a tutti gli obblighi di segretezza necessari;

 si deve prestare la massima attenzione alla conservazione e segretezza della propria password, evitando di comunicarla ad altri ed avendo cura di modificarla periodicamente;

 le prescrizioni tecniche individuate e comunicate dal gestore in ordine ai criteri di composizione della password vanno attentamente adempiute. In particolare, la password non deve contenere riferimenti agevolmente riconducibili all'addetto ed è modificata da quest'ultimo al primo utilizzo e successivamente, almeno ogni sei mesi o nel termine più breve individuato dal gestore informatico o qualora si abbiano sospetti che la password sia stata conosciuta da altri;

 in caso di trattamento di dati sensibili o giudiziari, la password è cambiata almeno ogni 3 mesi;

 qualora l'addetto al trattamento dei dati personali su una determinata postazione di lavoro venga trasferito ad altro ufficio o destinato ad altri compiti, si applica quanto contenuto nella nota della Direzione generale per i sistemi informativi prot. 1129 del 21 marzo 2006, nella quale è evidenziata l'opportunità che la postazione segua l'utente stesso. I dati devono, quindi, essere trasferiti sulla postazione del nuovo addetto, adottando tutte le misure idonee a garantire l'integrità dei dati e prestando particolare attenzione alla

cancellazione dei dati dalla postazione del precedente addetto. Nell'ipotesi, invece, che l'addetto al trattamento dei dati personali su una determinata postazione di lavoro venga sostituito senza trasferimento della postazione (ad esempio, nel caso di trasferimento ad altra amministrazione, di pensionamento, ecc.), il nuovo addetto deve essere dotato di nuove credenziali (username e password). A tal fine la richiesta va inoltrata al gestore del sistema informativo;

 gli addetti hanno cura di effettuare il salvataggio dei dati con frequenza almeno settimanale e di conservare il supporto informatico su cui è stato effettuato il salvataggio in luogo sicuro e protetto.

 Nel caso in cui venga utilizzata una postazione multimediale al di fuori degli uffici di segreteria (es. nei plessi….ect) l'incaricato al trattamento deve cancellare il file relativo ai dati trattati e/o copiarlo in apposito supporto esterno. In ogni caso anche i computer delle postazione dei plessi (in uso docenti…) debbo essere dotati di password di account o equivalente

Non è consentito effettuare:
 copie su supporti magnetici o trasmissioni non autorizzate dal Dirigente di dati oggetto del trattamento;

 copie fotostatiche o di qualsiasi altra natura, non autorizzate dal Dirigente, di stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento;

 sottrarre, cancellare, distruggere, senza l'autorizzazione del Dirigente, stampe, tabulati, elenchi, rubriche e ogni altro materiale riguardante i dati oggetto del trattamento;

 consegnare a persone non autorizzate dal Dirigente stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento.

**In caso di trattamento di dati sensibili e giudiziari con l'ausilio di strumenti elettronici** vengono adottate le seguenti, ulteriori, misure di sicurezza:

☐ i Dirigenti nominano con atto formale gli incaricati al trattamento di dati sensibili e giudiziari;

 i supporti rimovibili su cui sono memorizzati i dati sono custoditi dagli incaricati in luogo sicuro e protetto, al fine di evitare accessi non autorizzati e trattamenti non consentiti;

 i supporti rimovibili contenenti dati sensibili e giudiziari non utilizzati sono distrutti o resi inutilizzabili attraverso la cancellazione dei dati medesimi, che non consenta in alcun modo il loro recupero;

 in caso di danneggiamento dei dati o degli strumenti elettronici utilizzati per il trattamento, l'incaricato garantisce il ripristino dell'accesso ai dati in tempi certi, compatibili con i diritti degli interessati, e non superiori ai 7 giorni;

## 2) TRATTAMENTO SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

 Il dirigente e/o il responsabile della sicurezza nomina con atto formale gli incaricati al trattamento, impartendo loro idonee istruzioni.

 Agli incaricati è fornita adeguata formazione a cura dei competenti uffici, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime da adottare.

 I documenti che contengono dati sensibili o giudiziari debbono essere custoditi dagli incaricati fino alla restituzione, in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

 i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici non devono essere portati al di fuori dei locali individuati per la loro conservazione, se non in casi del tutto eccezionali e, nel caso questo avvenga, l'asportazione deve essere ridotta al tempo minimo necessario per effettuare le operazioni di trattamento;

 per tutto il periodo in cui i documenti contenenti i dati personali sono al di fuori dei locali individuati per la loro conservazione, l'incaricato del trattamento non deve lasciarli mai incustoditi;

 l'incaricato del trattamento deve inoltre controllare che i documenti contenenti i dati personali, composti da numerose pagine o più raccoglitori, siano sempre completi e integri;

 al termine dell'orario di lavoro l'incaricato del trattamento deve riportare tutti i documenti contenenti i dati personali nei locali individuati per la loro conservazione;

 i documenti contenenti i dati personali non devono essere mai lasciati incustoditi sul tavolo durante l'orario di lavoro;

 si deve adottare ogni cautela per evitare che persone non autorizzate vengano a conoscenza di documenti contenenti dati personali;

 per evitare il rischio di diffusione dei dati personali, si deve limitare l'utilizzo di copie fotostatiche;

 particolare cautela deve essere adottata quando i documenti sono consegnati in originale ad un altro incaricato debitamente autorizzato;

 i documenti contenenti dati personali sensibili o dati che, per una qualunque

ragione siano stati indicati come meritevoli di particolare attenzione, devono essere custoditi con molta cura.

**Non è consentito:**
☐ fare copie fotostatiche o di qualsiasi altra natura, non autorizzate dal Dirigente, di stampe, tabulati, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento;

 sottrarre, cancellare, distruggere, senza l'autorizzazione del Dirigente, stampe, tabulati, elenchi, rubriche ed ogni altro materiale riguardante i dati oggetto del trattamento;

 consegnare, a persone non autorizzate dal Dirigente, stampe, tabulati, elenchi, rubriche ed ogni altro materiale riguardante i dati oggetto del trattamento.

 E', inoltre, tassativamente proibito utilizzare copie fotostatiche di documenti all'esterno del posto di lavoro;

 è proibito discutere, comunicare o comunque trattare dati personali per telefono, se non si è certi che il destinatario sia un incaricato autorizzato a poter trattare i dati in questione;

 si raccomanda vivamente di non parlare mai ad alta voce, trattando dati personali per telefono, soprattutto utilizzando apparati cellulari, in presenza di terzi non autorizzati, per evitare che i dati stessi possano essere conosciuti, anche accidentalmente. Dette precauzioni assumono particolare importanza quando il telefono è utilizzato in luogo pubblico o aperto al pubblico.

**Controllo degli accessi**
L'accesso agli archivi contenenti dati personali, sensibili o giudiziari deve essere controllato.
Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, debbono essere identificate e registrate nell'apposito registro che viene istituito e tenuto presso il Plesso della sede centrale.