S C U O L A S E C O N D A R I A D I I° G R A D O “ Giuseppe GARIBALDI”

76015 Trinitapoli (BT) - Via Pirandello, 19 Cod. Mecc.: FGMM113004 – C.F.: 81004010716

Tel. e Fax: 0883/631182 E-mail: fgmm113004@istruzione.it web: www.scuolagaribaldi.eu

Posta Certificata: FGMM113004@PEC.ISTRUZIONE.IT

Prot. n. 504/Fp Trinitapoli, 22/02/2013

AL PERSONALE DOCENTE

SEDE

OGGETTO: Incarico per il trattamento dati
D.Lgs. 30 giugno 2003, n. 196 “Codice in materia di protezione dei dati personali”;
“Allegato B”: “Disciplinare tecnico in materia di misure minime di sicurezza”

IL RESPONSABILE DEL TRATTAMENTO DEI DATI

VISTO il D.Lgs. 30 giugno 2003, n. 196 “Codice in materia di protezione dei dati personali” e l’Allegato B: “Disciplinare tecnico in materia di misure minime di sicurezza”;

PREMESSO CHE

- la Legge sulla Privacy (D.Lgs. 30 giugno 2003, n. 196) ha disposto che il personale che presta l’attività a favore del titolare può accedere ai dati personali se incaricato per iscritto di compiere le operazioni del trattamento dal titolare o dal responsabile, e semprechè operi sotto la loro diretta autorità *(art. 30 comma 1,* D.Lgs. 30 giugno 2003, n. 196*).* Lo stesso articolo dispone inoltre che gli incaricati del trattamento devono elaborare i dati personali ai quali hanno accesso attenendosi alle istruzioni del Titolare o del Responsabile;
- lo scrivente, nominato dal *Titolare del Trattamento dei dati personali* quale *Responsabile del Trattamento dei dati personali*, conformemente a quanto stabilito dal D.Lgs. 30 giugno 2003, n. 196;
- ai sensi dell’art. 30 del Codice, è necessario procedere alla nomina di “Incaricati del trattamento dei dati personali” e ciò può avvenire anche mediante l’individuazione di unità organizzative alle quali i singoli dipendenti sono assegnati;
- in relazione al rapporto di lavoro con Lei in essere, con la presente;

DESIGNA

l’unità organizzativa **CORPO DOCENTI** quale

RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI

presenti nei nostri archivi, relativamente a:

1. dati degli alunni e loro famiglie per:
   a) attività di supporto alla didattica;
   b) attività integrative e complementari;
   c) attività generali riguardanti la didattica.
2. dati dei dipendenti:
   a) attività generali riguardanti la didattica, l’organizzazione e il funzionamento della scuola.

Nell’effettuare il trattamento dei dati personali devono essere soddisfatti i principi contenuti nella precitata normativa in materia di privacy e di sicurezza dei dati personali trattati.

In tale ambito, dovrà attenersi alle seguenti disposizioni:

1. Di dare atto che ogni dipendente che cessa l’attività lavorativa cessa automaticamente dalla funzione di Incaricato.
2. I dati personali devono essere esatti e, se necessario, aggiornati nonché pertinenti,

completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;

3. Il trattamento deve avvenire in modo lecito e secondo correttezza.
4. La raccolta e registrazione dei dati stessi deve avvenire per scopi determinati, espliciti e legittimi, e l'utilizzo dei dati deve avvenire per finalità non incompatibili con tali scopi.
5. La conservazione deve avvenire per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.
6. Nello svolgimento delle sue mansioni voglia adottare idonee misure di custodia e di controllo ed in genere qualunque accorgimento che consenta di ridurre al minimo i rischi di distruzione o perdita, anche accidentale dei dati stessi e che consenta di ridurre al minimo i rischi di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta e voglia osservare le procedure appositamente approntate per evitare quanto detto.
7. 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.

Le ricordiamo che l'Allegato B del Codice Unico prevede particolari regole alle quali ogni incaricato dovrà attenersi nel trattamento dei dati personali medesimi, regole che vengono riportate nel seguente Allegato "REGOLE PER IL TRATTAMENTO DEI DATI PERSONALI" e che dovranno da Lei essere osservate adeguandolo al suo profilo professionale.

Il Responsabile del Trattamento dei dati

IL DIRIGENTE SCOLASTICO
Prof. Giuseppe Luigi PIAZZOLLA

_____

L'incaricato del Trattamento dichiara di essere a conoscenza di quanto stabilito dall'Allegato B del Codice Unico e si impegna, nel trattamento dei dati personali ai quali è stato autorizzato ad accedere, ad attenersi alle regole qui indicate comprese quelle di cui all'Allegato "REGOLE PER IL TRATTAMENTO DEI DATI PERSONALI".

ALLEGATO
REGOLE PER IL TRATTAMENTO DEI DATI PERSONALI

Nell'effettuare trattamenti dei dati personali con strumenti diversi da quelli elettronici o comunque automatizzati (cioè nell'accedere ad archivi cartacei o nell'effettuazione di trattamenti manuali) dovrà attenersi a quanto segue a tutela dei diritti degli interessati ai quali si riferiscono i dati personali:

a) potrà accedere ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti a Lei assegnati;
b) gli atti e i documenti contenenti i dati personali, in azienda, saranno conservati in archivi ad accesso selezionato; dovranno quindi essere da Lei osservate le regole e le procedure per l'accesso selezionato; nel caso gli atti o i documenti riguardassero dati sensibili di cui all'art. 4, lett. d o di provvedimenti giudiziari di cui all'art. 4 lett. e del Codice Unico, oltre a quanto appena esposto, l'accesso agli archivi dei documenti contenenti i dati predetti sarà controllato e nel caso in cui dopo l'orario di chiusura degli archivi stessi Le venisse consentito l'accesso agli archivi medesimi dovrà seguire la specifica procedura che prevede preventivamente che i soggetti ammessi siano identificati e registrati;
c) nel caso in cui gli atti e i documenti contenenti i dati personali venissero a Lei affidati, dovranno essere da Lei conservati e restituiti al termine delle operazioni affidate; nel caso gli atti o i documenti riguardassero dati sensibili o provvedimenti giudiziari, oltre a quanto appena esposto, dovrà inoltre curare che gli atti e i documenti contenenti i dati sensibili o processuali predetti siano da Lei controllati e custoditi, fino alla restituzione, in maniera che ad essi non accedano persone prive di autorizzazione;
d) i supporti non informatici contenenti la riproduzione di informazioni relative al trattamento di dati personali sensibili e giudiziari devono essere conservati e custoditi con le modalità appena sopra esposte.

Nell'effettuare trattamenti dei dati personali con strumenti elettronici o comunque automatizzati dovrà attenersi a quanto segue:

a) sarà prevista una Parola chiave (*Password)* per l'accesso ai dati, a Lei fornita (che dovrà essere almeno di otto caratteri, se il sistema lo consente, e tenere strettamente riservata);
b) se tecnicamente possibile in relazione alle caratteristiche dell'elaboratore, sarà consentita l'autonoma sostituzione, ma in tale caso sarà necessario che Lei comunichi preventivamente la nuova *Password all'incaricato alla custodia delle Password* più sotto indicato (in busta chiusa mantenendo la riservatezza per la stessa); se la password si memorizza nell'archivio dell'elaboratore la sua memorizzazione equivarrà a comunicazione;
c) dovrà utilizzare un codice identificativo personale (ID USER) per l'utilizzazione di tutti gli elaboratori;
d) il codice identificativo personale (ID USER) sarà assegnato e gestito in modo che ne sia prevista la disattivazione in caso di perdita della qualità che consentiva l'accesso all'elaboratore o di mancato utilizzo del medesimo per un periodo superiore ai sei mesi.
e) gli elaboratori saranno protetti da *software antivirus* idoneo; nel caso in cui riscontrasse la presenza di virus in file presenti negli archivi degli elaboratori o su supporti magnetici, voglia adottare le procedure per eliminare o neutralizzare il file infetto ed avvisare l'Amministratore di sistema.
f) l'accesso per effettuare le operazioni di trattamento sarà consentito solo sulla base di autorizzazioni assegnate, singolarmente o per gruppi di lavoro, agli incaricati; dette autorizzazioni all'accesso sono rilasciate e revocate dal Titolare o dal Responsabile del Trattamento dei dati personali; ancorché Lei venisse a ciò autorizzato, anche se sarà espressamente precisato nell'autorizzazione stessa, già sin d'ora si precisa che l'autorizzazione sarà comunque da intendersi limitata ai soli dati la cui conoscenza è necessaria e sufficiente per lo svolgimento delle operazioni di trattamento o di manutenzione; la validità delle richieste di accesso ai dati personali sarà verificata dalle persone preposte o automaticamente dal software prima di consentire l'accesso stesso e periodicamente, comunque almeno una volta l'anno, sarà verificata la sussistenza delle condizioni per la conservazione delle singole autorizzazioni in essere;
g) non è consentita l'utilizzazione di un medesimo codice identificativo personale per accedere contemporaneamente alla stessa applicazione da diverse stazioni di lavoro;
h) nel caso di trattamento dei dati sensibili o giudiziari effettuato con elaboratori elettronici, i

supporti già utilizzati per il trattamento potranno essere riutilizzati qualora le informazioni precedentemente contenute non siano tecnicamente in alcun modo recuperabili, altrimenti dovranno essere distrutti;

i) nel caso di trattamento di dati idonei a rivelare lo stato di salute e la vita sessuale effettuato con elaboratori elettronici da parte di organismi sanitari saranno adottate tecniche di cifratura o di codici identificativi per separare tali dati dagli altri personali dell'interessato.

MANSIONARIO
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;
- in caso di assenza temporanea l'addetto deve chiudere o spegnere o disattivare la postazione. Nel caso, invece, di assenza prolungata dell'addetto il 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
- 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. n. 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.

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;
- sono individuate le postazioni di lavoro adibite 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;
- per i dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24 del Disciplinare tecnico, devono essere adottati criteri specifici per la cifratura o per la

separazione di tali dati dagli altri dati personali dell'interessato.

TRATTAMENTO SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

Norme di sicurezza per gli incaricati del trattamento di dati personali effettuato senza l'ausilio di strumenti elettronici:

In base a quanto stabilito dal punto 27 e dal punto 28 del Disciplinare tecnico in materia di misure minime di sicurezza (allegato B al D.Lgs. n. 196 del 30 giugno 2003), per i trattamenti di dati personali effettuati senza l'ausilio di strumenti elettronici vengono stabilite le seguenti regole che gli incaricati del trattamento debbono osservare:

- 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;
- 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 effettuare:

- 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.
- è, 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.