MINISTERO DELL'ISTRUZIONE DELL'UNIVERSITA' E DELLA RICERCA

C.P.I.A. REGGIO NORD

(Centro Provinciale per l'Istruzione degli Adulti)

Via Conte Ippolito, 22 – 42015 Correggio (RE)

codice fiscale: 91171510356 - Tel. 0522 633059

e-mail: remm133007@istruzione.it - PEC: remm133007@pec.istruzione.it

www.cpiareggionord.gov.it

C.P.I.A. Reggio Nord

Prot.n.8048/A32d

Correggio, 21 dicembre 2016

All'Albo
Al DSGA
Agli Assistenti Amministrativi
Al collaboratore del Dirigente

Oggetto: **Allegato 5 – Misure di protezione dati** (D. Lgs. n. 196/2003 - Privacy)

Indice:

1 - Regole generali del 'Codice in materia di protezione dei dati personali' D.Lgs 196/2003

Queste Istruzioni vanno applicate da tutte le categorie di Incaricati

Art. 31. Obblighi di sicurezza

1. I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Art. 34. Trattamenti con strumenti elettronici

1. Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:

autenticazione informatica;

a) adozione di procedure di gestione delle credenziali di autenticazione;
b) utilizzazione di un sistema di autorizzazione;
c) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli Incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
d) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
e) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
f) tenuta di un aggiornato documento programmatico sulla sicurezza;
g) adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.

Art. 35. Trattamenti senza l'ausilio di strumenti elettronici

1. Il trattamento di dati personali effettuato senza l'ausilio di strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:

a) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli Incaricati o alle unità organizzative;
b) previsione di procedure per un'idonea custodia di atti e documenti affidati agli Incaricati per lo svolgimento dei relativi compiti;
c) previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli Incaricati.

ELENCO MISURE DI PROTEZIONE CHE GLI INCARICATI DEVONO ATTUARE

(nel caso di impossibilità devono comunicarlo al Titolare o al Responsabile se esiste)

Va ricordato che il D.Lgs 196/2003 sancisce il dovere di **mantenere integri i dati** forniti dall'interessato finché non siano più necessari. Pertanto tra le misure di protezione dei dati vanno considerate anche quelle mirate a questo scopo (protezione degli archivi cartacei da furti, incendi ed altri eventi distruttivi; protezione degli archivi elettronici da sbalzi di corrente o eventi che danneggino il computer o le sue memorie, effettuazione di copie di sicurezza degli archivi elettronici con periodicità adeguata, ecc.)

2 - Trattamenti dei dati personali su supporto cartaceo

Queste Istruzioni vanno applicate dalla categoria: Assistenti Amministrativi e DGSA, Collaboratori Scolastici per quanto di loro pertinenza.

Vanno lette per necessaria conoscenza dalle seguenti categorie: Collaboratori del Dirigente, Collaboratori Scolastici in quanto di supporto alla Segreteria

- **Procedura di Protezione Dati PP01: documenti in ingresso**

Per "documenti in ingresso", si intendono i documenti o i supporti contenenti dati personali acquisiti dalla scuola ai fini di un loro impiego in trattamento.

Relativamente al trattamento dei documenti in ingresso, è necessario adottare le cautele seguenti:

- i documenti in ingresso devono essere utilizzati soltanto da chi sia Incaricato al trattamento dei dati che contengono o dal Responsabile;
- l'Incaricato deve verificare:
  - la provenienza dei documenti;
  - che tali documenti siano effettivamente necessari al trattamento in questione;
  - la tipologia dei dati contenuti (comuni, sensibili, giudiziari o altri dati particolari), al fine di individuare le modalità legittime ed idonee per il trattamento e le misure di sicurezza da attuare;
  - l'osservanza del principio di pertinenza e non eccedenza rispetto o alle finalità del trattamento, la completezza, la correttezza e l'aggiornamento dei dati.

Tutti i documenti in ingresso e in uscita vengono protocollati (gestione di dati comuni, particolari, sensibili, giudiziari).

I documenti cartacei in ingresso vengono consegnati al DSGA che provvede a designarne la destinazione; nei casi di documenti con dati riservati o sensibili, il DSGA li consegna direttamente al Dirigente o, in sua assenza, li inserisce in busta chiusa portandoli poi all'attenzione del Dirigente stesso.

Ogni documento cartaceo riservato in ingresso ricevuto tramite posta o ricevuto in busta chiusa consegnata a mano viene di norma consegnato chiuso direttamente al Dirigente Scolastico.

I documenti protocollati vengono poi passati all'Incaricato che deve trattare la pratica, che si occupa anche dell'archiviazione o della spedizione.

I dati neutri (ad es.: ricevute di pagamenti, domande di certificazioni, …), vengono trattati direttamente dalla segreteria.

I fonogrammi vengono trascritti e trattati come un documento cartaceo ricevuto.

- **Procedura di Protezione Dati PP02: documenti in uscita**

Per "documenti in uscita", si intendono i documenti o i supporti contenenti dati personali prodotti e rilasciati dalla scuola a soggetti esterni alla stessa.

L'Incaricato del trattamento deve trattare qualunque prodotto dell'elaborazione di dati personali, ancorché non costituente documento definitivo, (appunti, stampe interrotte, stampe di prova, ecc.) con le stesse cautele che sarebbero riservate alla versione definitiva.

Nel caso di documenti in uscita è necessario all'atto della consegna o dell'invio, verificare che la persona che riceve il documento sia legittimata al ritiro e all'utilizzo (delega).

- **Procedura di Protezione Dati PP03: verifica della legittimità del trattamento in corso**

Di fronte a qualsiasi nuovo trattamento di dati, il Responsabile del trattamento stesso e l'Incaricato devono chiedersi se rientra nel preciso recinto di legittimità, delimitato dai seguenti paletti:

Il trattamento sia connesso con **l'esercizio delle funzioni istituzionali** (principio di **pertinenza)** e che esse non siano perseguibili attraverso il trattamento di dati anonimi.

1. Le modalità del trattamento siano tali da determinare il minimo sacrificio possibile del diritto alla riservatezza dell'Interessato (principio di **non eccedenza:** è illegittimo chiedere un dato in più di quello che è strettamente necessario).
2. Ogni fase del trattamento rispetti **le norme di legge e di regolamento.**
3. In ogni fase del trattamento siano adottate le **misure di sicurezza previste per la categoria alla quale il dato appartiene**
4. Se il dato è sensibile o giudiziario, siano rispettati i presupposti per avere la legittimazione a trattarlo
5. In caso di comunicazione o diffusione, che il dato rientri nelle categorie autorizzate

- **Procedura di Protezione Dati PP04: quando un alunno o un dipendente ci lascia definitivamente**

Gli vanno *consegnati tutti i documenti contenenti dati personali* che la scuola non sia obbligata a conservare. Nel caso non fosse possibile trattare direttamente con l'Interessato, si deve mandare un *avviso per il ritiro*. Nel frattempo i materiali da consegnare vanno *posti in busta chiusa*. Al ritiro va fatta *firmare una ricevuta*. In ogni caso qualunque fascicolo personale che transiti dall'archivio corrente a quello storico, deve essere prima depurato di tutti dati personali non più necessari.

- **Procedura di Protezione Dati PP05: trattamento appena un documento viene ricevuto**

L'Incaricato che riceve "brevi manu" allo sportello o in qualsiasi altro punto della scuola documenti contenenti *dati*

personali di tipo sensibile, giudiziario o particolare ad alto livello di delicatezza ancora non collocati in busta chiusa, deve immediatamente metterli *in busta chiusa* e inserirli nella posta in arrivo per il Dirigente Scolastico.

- **Procedura di Protezione Dati <u>PP06: circoscrivere al massimo il numero di Incaricati che trattano una pratica</u>**

I documenti contenenti dati personali di tipo sensibile, giudiziario o particolare ad alto livello di delicatezza, devono essere visti e conosciuti dal minor numero possibile di Incaricati.

- **Procedura di Protezione Dati <u>PP07: affidamento all'Incaricato sotto la sua responsabilità</u>**

In generale qualsiasi documento o fascicolo contenente dati personali va trattenuto dall'Incaricato per il tempo strettamente necessario alla lavorazione e riposto nel suo archivio appena terminato il lavoro o alla fine della giornata lavorativa. <u>Non devono essere lasciati sui tavoli o comunque fuori dai contenitori documenti o fascicoli contenenti dati personali.</u>

Nei casi in cui i documenti con dati sensibili/giudiziari debbano essere trattati per un certo periodo di tempo, vengono mantenuti sotto la responsabilità dell'Incaricato per il più breve tempo possibile. L'Incaricato ha istruzione di elaborare le pratiche riferite a questi documenti in modo che nessun altro possa sbirciarli o tanto meno trovarli momentaneamente abbandonati sul tavolo; nei momenti di non utilizzazione di conservarli chiusi a chiave.

- **Procedura di Protezione Dati <u>PP08: Regole generali per la sicurezza degli archivi</u>**

Vanno poste in essere le misure necessarie a ridurre al minimo i rischi di:

- accesso fisico non autorizzato;
- furto o manomissione dei dati da parte di malintenzionati;
- distruzione o perdita dei dati dovuta ad eventi fisici;
- perdita accidentale dei dati.

Gli archivi possono essere soltanto di due tipi:

1) a **bassa sicurezza**, per dati comuni o neutri, con accesso "selezionato" (= il Titolare o il Responsabile decidono chi può entrarvi e gli danno la chiave personale o mettono a disposizione la chiave in modo che solo costoro possono utilizzarla). Il Responsabile deve assicurarsi che esista un numero definito di chiavi e che la chiave di riserva sia chiusa in luogo ben protetto.
2) ad **alta sicurezza**, ovviamente per *dati sensibili o giudiziari*, con *accesso non solo selezionato, ma anche "controllato":* c'è una sola chiave disponibile, l'Incaricato che ne ha bisogno e che è autorizzato deve chiederla al "Responsabile delle chiavi". Il Dirigente Scolastico, in quanto Titolare, ha libertà assoluta di accesso.

Dati personali comuni - protezione dall'accesso fisico non autorizzato: i documenti contenenti dati personali comuni sono conservati in archivi ad accesso selezionato: pertanto l'accesso ai dati è consentito ai soli Incaricati del trattamento.

I documenti possono essere estratti dall'archivio e affidati alla custodia dell'Incaricato del trattamento per il tempo strettamente necessario al trattamento medesimo: egli ha cura di garantirne la riservatezza e provvede al deposito in archivio al termine delle operazioni. Il Responsabile verifica che la dotazione di arredi (cassettiere, armadi ecc.) muniti di meccanismi di serratura adatta a garantire la sicurezza sia adeguata, altrimenti deve segnalare al Titolare la necessità di acquisirli.

Dati sensibili e giudiziari - protezione dall'accesso fisico non autorizzato**:** l'accesso è limitato agli Incaricati del trattamento. Gli archivi devono essere ad accesso controllato. Tali documenti devono essere conservati in elementi di arredo (armadi o cassettiere) muniti di serratura a chiave.

Protezione dei locali archivio contenenti dati personali sensibili:

- se i documenti contenenti dati personali sensibili sono archiviati in arredi (armadi o cassettiere) chiusi a chiave, l'accesso ai locali che li contengono può non essere soggetto a particolari restrizioni. Resta fermo l'obbligo per l'Incaricato e il Responsabile di verificare che gli elementi di arredo siano sempre chiusi e che vengano rispettate le misure relative alla gestione delle chiavi;
- se non c'è immediata disponibilità di arredi muniti di serratura per l'archiviazione dei documenti contenenti dati personali sensibili, gli archivi devono in ogni caso essere ubicati in appositi locali chiusi a chiave e il più possibile protetti dall'intrusione dall'esterno. In tal caso il personale diverso dagli Incaricati del trattamento che vi accede deve essere accompagnato da uno dei soggetti Incaricati del trattamento o dal custode delle chiavi, che deve verificare che non avvenga un accesso illecito ai dati sensibili ivi contenuti;
- ogni stanza-archivio deve essere chiusa a chiave quando non presenziata.

Protezione dal rischio di perdita dei dati dovuta ad eventi fisici

Un archivio è sottoposto al rischio di svariati tipi di eventi che possono provocare la distruzione o il danneggiamento dei documenti. Per ridurre al minimo questo rischio le principali misure da prendere sono le seguenti:

1) evitare eccessivi carichi d'incendio;
2) utilizzare il più possibile contenitori chiusi;
3) applicare in modo assoluto il divieto di fumo dentro la stanza e nelle adiacenze;
4) non lasciare pertugi dai quali possano essere gettati materiali o liquidi;
5) nelle vicinanze devono essere presenti idonei dispositivi antincendio.

Misure logistiche:

Il personale addetto al trattamento di dati personali deve porre in essere le misure necessarie a ridurre al minimo i rischi di: accesso fisico non autorizzato; furto o manomissione dei dati da parte di malintenzionati; distruzione o perdita dei dati dovuta ad eventi fisici; perdita accidentale dei dati.

Chiusura a chiave dei contenitori metallici.

Gli armadi e contenitori che ospitano archivi vanno chiusi a chiave alla fine della giornata lavorativa e le chiavi vanno messe in luogo sicuro indicato dal *Responsabile* o dal *Custode delle chiavi*. A fine giornata vanno chiusi a chiave anche le singole stanze che contengono dati (es. segreteria, presidenza, sala insegnanti, …).

- **Procedura di Protezione Dati <u>PP09: archiviazione separata</u>**

I documenti contenenti *dati sensibili, giudiziari o particolari ad alto livello di delicatezza* vanno di norma chiusi in busta di carta, su cui è riportato nome (o codice identificativo per dati particolarmente sensibili) dell'interessato, tipo di documento, data attuale (se non conoscibile, mettere una data presunta seguita da un punto interrogativo).

La busta viene archiviata in uno degli Armadi cosiddetti "dei Dati Protetti" (permanentemente chiuso a chiave).

Al posto del documento così protetto viene messo nel fascicolo un foglio con annotazione generica del tipo di documento e della sua collocazione.

- **Procedura di Protezione Dati PP10: conservazione di registri e altri documenti utilizzati per anni scolastici precedenti e non più utilizzati**

Conservazione: molti documenti e registri sono utilizzati per un intero anno scolastico ma solo in quello. Tra questi, i documenti non più utilizzati negli anni seguenti (salvo ricorsi o richieste di accesso legittime) al termine dell'anno scolastico sono impacchettati a gruppi omogenei e chiusi con carta e scotch; sull'involucro viene riportato il contenuto e la scadenza per l'eliminazione. Vengono conservati in una stanza chiusa a chiave ad accesso selezionato. Il Responsabile dispone l'organizzazione delle operazioni. L'eliminazione dei documenti avviene mediante la Procedura *PP14*

- **Procedura di Protezione Dati PP11: archiviazione nel fascicolo personale**

I documenti non archiviati, finché l'alunno è iscritto o il dipendente è in servizio, vengono conservati nel fascicolo personale. In particolare alcuni dati si situano in una zona di confine tra dato particolare e dato sensibile (ad es. certificati medici generici privi di diagnosi), data la loro bassa pericolosità vengono mantenuti nel fascicolo personale, ma in una cartella separata. Il fascicolo personale è conservato nel relativo archivio corrente chiuso a chiave negli orari non lavorativi, in una stanza che viene chiusa a chiave al di fuori dell'orario lavorativo.

- **Procedura di Protezione Dati PP12: archiviazione nell'archivio storico**

Quando l'alunno ha cessato la frequenza o il dipendente ha cessato di essere in carico alla scuola, il relativo fascicolo personale, depurato dei documenti non più necessari, viene archiviato nel corrispondente archivio storico, collocato in una stanza chiusa a chiave, ad accesso selezionato.

- **Procedura di Protezione Dati PP13: scarto periodico dei documenti**

Scarto periodico dei documenti contenenti dati personali di qualunque livello, ai sensi dell'art. 11 comma e del D.Lgs 196/2003, vanno eliminati non appena cessa lo scopo per cui sono stati raccolti. Pertanto periodicamente, all'inizio di ogni anno solare per le pratiche che hanno questa cadenza, oppure all'inizio di ogni nuovo anno scolastico vengono eliminati i documenti non più necessari, utilizzando una corretta procedura (*procedura PP14*).

- **Procedura di Protezione Dati PP14: distruzione dei documenti**

La distruzione di documenti contenenti dati personali di qualunque livello avverrà con modalità di Protezione Dati per impedire che estranei prendano visione del contenuto o, peggio, se ne impadroniscano. Di queste operazioni si occupano solamente Incaricati, con la qualifica di Collaboratori Scolastici e Assistenti Amministrativi. Se possibile si utilizza un apparecchio che trincia la carta. Altrimenti si provvede a rendere comunque anonimi mediante tagli e cancellature indelebili i documenti sensibili, giudiziari e particolari ad alto rischio. Per gli altri ci si assicurerà che nessuno possa impadronirsene prima della distruzione (o riciclo o conferimento in discarica) da parte dell'ente a cui si conferiranno.

- **Procedura di Protezione Dati PP15: appunti, bozze e copie superflue**

Anche gli appunti, le bozze, le stampe intermedie, le fotocopie superflue costituiscono elemento di rischio, pertanto essi vanno distrutti con la prescritta procedura o, se necessario conservarli, archiviati insieme all'originale del documento sensibile o giudiziario.

- **Procedura di Protezione Dati PP16: cautele nella fase di fotocopiatura**

Quando documenti contenenti dati personali di tipo sensibile, giudiziario o particolare ad alto livello di delicatezza devono essere fotocopiati, hanno la precedenza su tutti gli altri e devono essere adottate opportune cautele affinché nessun altro ne possa prendere visione. Tranne impossibilità tecnica, l'operazione di fotocopiatura deve essere effettuata dall'Incaricato che tratta la pratica. L'Incaricato deve fare in modo che il documento non venga lasciato in giacenza vicino alla fotocopiatrice né prima né dopo la fotocopiatura. L'incaricato provvede ad eliminare (secondo la *procedura PP08*) anche le eventuali copie non perfettamente riuscite.

- Procedura di Protezione Dati **PP17: la movimentazione da parte di terzi**

Quando documenti contenenti dati personali di tipo sensibile, giudiziario o particolare ad alto livello di delicatezza devono essere movimentati attraverso Collaboratori scolastici Incaricati, anche all'interno della scuola, devono essere collocati in busta chiusa. Anche la spedizione postale o la consegna in altro modo deve essere effettuata esclusivamente da Incaricati che abbiano ricevuto almeno l'autorizzazione a questo ambito di trattamento e che assicurino massima diligenza nella custodia dei plichi. Il Responsabile può autorizzare al trasporto da una sede all'altra anche personale docente a ciò disponibile.

- **Procedura di Protezione Dati PP18: ingresso di persone esterne per pulizia o manutenzione**

L'accesso di dipendenti o estranei per la manutenzione o la pulizia dei locali contenenti archivi cartacei o delle attrezzature in tali stanze contenute, deve essere effettuata solo con i contenitori chiusi a chiave. Se dati sensibili o giudiziari non sono chiudibili in contenitore, l'intervento deve essere effettuato esclusivamente alla presenza di un Incaricato del trattamento di tali dati.

- **Procedura di Protezione Dati PP18 bis: ingresso di altre persone in segreteria**

Di norma l'ingresso in segreteria, nelle ore lavorative, è riservato a chi vi lavora, al Dirigente e ai suoi collaboratori, ai Collaboratori scolastici che ne hanno motivo. Gli altri dipendenti e gli estranei di norma non possono accedere, salvo che ne facciano richiesta preventiva e ne ottengano l'autorizzazione di volta in volta.
Ciò viene previsto allo scopo di evitare che persone non autorizzate vedano anche involontariamente documenti riservati.
La segreteria deve essere chiusa a chiave quando non è presenziata da chi vi lavora. Possibilmente le pulizie devono essere organizzate in orari in cui vi sia almeno un Assistente Amministrativo presente.

3 - Trattamenti con strumenti elettronici

*Queste Istruzioni vanno **applicate** dalla categoria: **Assistenti Amministrativi e DSGA**, **Coll. Scolastici** per quanto di loro pertinenza.*
*Vanno **lette** per necessaria conoscenza dalle seguenti categorie: **Collaboratori del Dirigente**, **Collaboratori Scolastici** in quanto di supporto alla Segreteria*

- **Procedura di Protezione Dati PP19: sistema di autorizzazione dell'accesso**

1. Il trattamento di dati personali con **strumenti elettronici** é consentito esclusivamente agli Incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.
2. Le ***credenziali di autenticazione*** consiste un codice per l'identificazione dell'Incaricato (user-id o username o `nome

utente') fisso e parzialmente riservato, cui è associata una password segreta variabile.
3. Ad ogni Incaricato sono assegnate individualmente una o più credenziali per l'autenticazione.
4. Ogni Incaricato deve adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale (= password segreta).
5. La *parola chiave*, quando é prevista dal sistema di autenticazione, dev'essere composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito. Essa non deve contenere riferimenti agevolmente riconducibili all'Incaricato (nomi o iniziali proprie o di parenti, date di nascita, e simili). La parola chiave deve essere modificata da ciascun Incaricato al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave deve essere modificata almeno ogni tre mesi.
6. Le credenziali di autenticazione non utilizzate da almeno sei mesi vanno disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
7. Le credenziali vanno disattivate anche in caso di perdita della qualità che consente all'Incaricato l'accesso ai dati personali.
8. Gli Incaricati non devono lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.
9. Non appena un Incaricato modifica la parola chiave, deve scriverla in un foglio, chiuderla in busta chiusa (all'esterno indicare "parola chiave del sig. … per il computer … e la data). La busta va data al DGSA o al "Custode delle Password" (se nominato), che la custodisce chiusa a chiave.
10. Ovviamente le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione o all'uso personale o didattico.
    N.B.: *costituisce infrazione disciplinare gravissima scrivere una password o una user-id su fogli di carta o quaderni, tanto peggio se in vicinanza del computer. Se non si può memorizzarla, è consentito soltanto conservarla dentro il portafoglio, meglio se mascherata premettendo e posponendo un certo numero di lettere o cifre.*

Sistema di autorizzazione

Il Responsabile individua quali profili di autorizzazione sono necessari per gli Incaricati che utilizzano il computer. In pratica stabiliscono quali computer può usare ogni Incaricato, di quali cartelle (directories) ha necessità, quali altre cartelle vanno create, a quali cartelle possono accedere tutti gli Incaricati e a quali possono accedere solo alcuni e a quali soltanto un singolo Incaricato, quali devono essere cifrate e con quale tecnica.
L'Amministratore di sistema o un tecnico dovrà tradurre in pratica queste direttive, costruendo i necessari profili di autorizzazione differenziati per ciascun utilizzatore, al quale sarà consegnata la corrispondente credenziale di autenticazione (più d'una se necessario).
L'Amministratore di sistema o un tecnico dovrà provvedere anche a tradurre in pratica operativamente le altre indicazioni strategiche sulla gestione dei programmi e dei loro aggiornamenti, del backup, dell'antivirus, del firewall (protezione dagli accessi tramite internet) e dei sistemi di ripristino dati in caso di "disastro informatico".

- **Procedura di Protezione Dati <u>PP20: salvataggio dei dati (back-up)</u>**

Il Responsabile è tenuto a salvare i dati con frequenza almeno settimanale (lo dice il Codice). Pertanto procederà al back-up su appositi dispositivi di back-up supporti magnetici che verranno riposti nell'armadio protetto di cui è responsabile il DGSA e che deve restare sempre chiuso.

- **Procedura di Protezione Dati <u>PP21 - Ulteriori misure in caso di trattamento di dati sensibili o giudiziari: Programmi firewall, dispositivi firewall</u>**

Accessi abusivi logici (cioè eseguiti attraverso la logica del software)

I dati devono essere permanentemente protetti contro l'accesso abusivo, di cui all'art. 615-ter del codice penale (accesso abusivo per via telematica da parte di persone molto esperti nell'utilizzare la connessione a Internet per introdursi nei computers durante il collegamento e copiare dati o manometterli).
Molto utile è l'aggiornamento frequente del Sistema Operativo. La protezione da queste "intrusioni logiche" viene effettuata con un apposito "*firewall*" che intercetta ogni utilizzo delle porte di comunicazione del computer sia in entrata che in uscita e verifica se è autorizzato altrimenti lo blocca e chiede di autorizzare o meno la comunicazione.

- **Procedura di Protezione Dati <u>PP22 - Ulteriori misure in caso di trattamento di dati sensibili o giudiziari : Programmi antivirus</u>**

I dati devono essere permanentemente protetti contro virus e altri programmi informatici che possono causare perdita di dati, malfunzionamenti, danni all'hardware, trasmissione all'esterno di files contenuti nel computer. La protezione viene effettuata mediante l'utilizzo di un programma antivirus. Il programma antivirus deve essere aggiornato frequentemente, almeno ogni settimana (la norma prevede almeno 6 mesi, ma è sicuramente insufficiente, visto che ogni giorno nascono nuovi virus). Il DSGA organizza e verifica che queste condizioni siano attuate oltre ad eseguire quanto è di sua pertinenza. Prima di aprire ciascun messaggio di posta elettronica l'Incaricato è tenuto a valutare se il messaggio proviene da mittente noto o plausibile, in caso contrario deve adottare particolari cautele. Non deve aprire allegati che abbiano estensione ".exe", ".pif", ".scr" a meno che non sia sicuro del mittente; se l'estensione appare doppia (esempio: "pif.scr" non deve aprire comunque l'allegato). Inoltre deve valutare dal titolo dell'allegato se esso è plausibile e pertinente col mittente e con le attività di interesse della scuola.

- **Procedura di Protezione Dati <u>PP23: uso dei supporti rimovibili</u>**

I floppy disk e i CD non devono essere utilizzati mai per memorizzare i file contenenti dati personali; tali files vanno invece memorizzati solo nel disco fisso di computer protetti da sistema di credenziali di accesso. Ciò al fine di evitare che chi si impadronisca di tali supporti rimovibili, possa accedere ai dati. I supporti rimovibili devono essere utilizzati esclusivamente per le copie di sicurezza (back-up) e subito devono essere riposti nel luogo sicuro indicato.

- **Procedura di Protezione Dati <u>PP24</u>: <u>cautele nel riutilizzo dei supporti rimovibili</u>**

I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati devono essere distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri Incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili (= riformattando il disco e verificando l'avvenuta riformattazione)

- **Procedura di Protezione Dati <u>PP25 – accesso di manutentori software o hardware</u>**

Se soggetti esterni alla propria struttura attuano installazioni per le misure minime per la sicurezza informatica, per

provvedere alla esecuzione è assolutamente tassativo ricevere dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del disciplinare tecnico di cui allegato B del D.Lgs 196/2003. Tale dichiarazione va consegnata al titolare.
In caso di manutenzione dell'hardware o del software da parte di persone esterne alla scuola o comunque non incaricate del trattamento dei dati contenuti in quel computer, un Incaricato deve controllare a vista le operazioni eseguite, in modo da verificare che non ci sia mai lettura o copia di dati né che siano indebitamente scoperte le parole chiave.

- **Procedura di Protezione Dati PP26: pulizia dei locali**

L'accesso di dipendenti o estranei per la pulizia dei locali contenenti dischi di back-up deve essere effettuata solo con i contenitori chiusi a chiave o alla presenza di un Incaricato del trattamento di tali dati. Durante l'accesso per la pulizia tutti i computer contenenti dati sensibili o giudiziari devono essere spenti o in modalità salvaschermo con password di ripristino oppure deve presenziare un Incaricato del trattamento di tali dati.

- **Procedura di Protezione Dati PP27: ingresso di persone esterne per manutenzione locali o impianti o attrezzature**

Stanze contenenti dischi di back-up: l'accesso di dipendenti o estranei per la manutenzione deve essere effettuato solo con i contenitori chiusi a chiave o alla presenza di un Incaricato del trattamento di tali dati. Durante l'accesso per l'intervento tutti i computer contenenti dati sensibili o giudiziari devono essere spenti oppure deve presenziare un Incaricato del trattamento di tali dati.

- **Procedura di Protezione Dati PP28:** procedure ad ogni **variazione degli Incaricati**

Se entra in servizio un Incaricato che ha accesso alle risorse informatiche il Responsabile deve provvedere a fare in modo che sia in grado di ottenere un sistema di credenziali.
Se un Incaricato che ha accesso alle risorse informatiche cessa dal servizio o è assente per più di 6 mesi, il Responsabile deve provvedere a fare in modo che sia annullato il suo sistema di credenziali.

- **Procedura di Protezione Dati PP29: scelta del software**

Nella scelta del software, va esplicitamente verificato se ogni programma è realizzato in modo da attuare le misure di sicurezza previste dal Codice. In particolare che sia consentito l'accesso multiplo basato su credenziali, che gli archivi siano cifrati, che i programmi che trattano sia dati non sensibili che dati sensibili siano in grado di archiviare questi ultimi a parte e non li renda visibili insieme agli altri dati, ma sia necessario accedere specificamente ad essi, eventualmente con una seconda protezione con credenziali. Va richiesta una dichiarazione di conformità al D.Lgs 196/2003.

- **Procedura di Protezione Dati PP30: accesso ai dati in assenza dell'Incaricato**

Qualora, in caso di assenza dell'Incaricato assegnatario della dotazione informatica, si renda necessario per ragioni improrogabili l'utilizzo di dati accessibili in via esclusiva con i suoi codici di accesso è necessario rispettare le seguenti regole:

1) deve sussistere un'improrogabile necessità di accedere ai dati per ragioni di servizio;
2) deve essere verificata l'impossibilità o la notevole difficoltà di raggiungere l'Incaricato;
3) il Responsabile (DGSA) apre la busta chiusa dov'è scritta la password poi la mette in una nuova busta chiusa. Chi ha aperto la busta, comunica l'accesso effettuato al dipendente assente al momento del suo rientro e lo invita a modificare immediatamente la password.

- **Procedura di Protezione Dati PP31: protezione dal furto di computer portatili** contenenti dati personali

Considerata la facilità con cui possono essere sottratti i computer portatili essi non devono essere utilizzati per dati sensibili o giudiziari. Vanno rigorosamente chiusi in armadio di sicurezza o cassaforte, quando non utilizzati, i computer portatili che contengono dati soggetti a tutela.

4 - Trattamenti da parte dei docenti

*Queste Istruzioni vanno **applicate** dalla categoria: **Docenti**.*
*Vanno **lette** per necessaria conoscenza dalle seguenti categorie: **Collaboratori del Dirigente**, **Collaboratori Scolastici** in quanto di supporto ai docenti*

- **Procedura di Protezione Dati PP32: registri**

I ***registri personali*** devono essere sempre custoditi in modo sicuro.
I ***registri di classe*** devono essere consultabili solo dagli alunni della classe interessata e si deve vigilare perché non vi siano accessi non autorizzati. I collaboratori scolastici sono Incaricati di riporli in luogo sicuro quando terminano le lezioni.
Il ***registro dei verbali del consiglio di classe*** e qualunque ***altro registro di verbali***, affidato per la scrittura, la firma o la consultazione al coordinatore di classe, deve essere mantenuto protetto da accessi non autorizzati e conservato in luogo sicuro ad opera del coordinatore stesso.

- **Procedura di Protezione Dati PP33: certificazioni mediche e informazioni sullo stato di salute degl alunni**

I dati personali in grado di rivelare lo ***stato di salute*** sono classificati "sensibili" e quindi protetti dalla visione di terzi che non sia strettamente necessaria. Quindi eventuali *certificati medici* vanno protetti dalla visione di terzi e consegnati al più presto in segreteria.
I *certificati di esonero o limitazione presentati per educazione fisica* debbono essere fatti recapitare in segreteria.
A volte l'insegnante ottiene informazioni su particolari, anche gravi, *problemi di salute* dell'alunno che possono presentarsi durante le lezioni, in alcuni casi con grave rischio per la vita dell'alunno (allergie con pericolo di shock anafilattico, asma grave, ecc.) o imbarazzanti (disturbi di continenza, ecc.), messe a disposizione dai genitori o dall'interessato. Se l'informazione è orale l'insegnante è tenuto al riserbo. Se esiste qualche comunicazione scritta, trattasi di dato sensibile e va trattato con particolari cautele, chiedendo al Titolare o al Responsabile come fare.
Anche informazioni su *particolari diete* seguite dall'alunno o per motivi di salute o per motivi religiosi sono da considerare dato sensibile, pertanto va rivelato soltanto nei casi strettamente necessari ed omettendone la ragione.
Nel caso di ***alunni portatori di handicap*** la visione e la detenzione della relativa documentazione per l'integrazione è un dato di massima sensibilità in quanto idoneo a rivelare lo stato di salute. Pertanto i documenti dovranno essere visti soltanto dai docenti e personale strettamente necessario, conservati con elevata cautela, poi consegnati in segreteria. Nei registri, nelle relazioni e nei PEI si riportano solo i dati indispensabili alla specifica funzione e l'annotazione del luogo di

conservazione dei dati sensibili, ai fini della possibilità di consultazione.

- **Procedura di Protezione Dati PP34: gestione di documenti scolastici**

In generale qualunque documento scolastico che contenga dati personali di qualcun altro è sottoposto dal D.Lgs 196/2003 a una qualche forma di protezione, quindi va custodito in modo che nessun altro possa visionarlo, copiarlo o impadronirsene. Se non c'è motivo di detenerlo, va riconsegnato in segreteria per l'archiviazione.

- **Procedura di Protezione Dati PP35: elaborati contenenti notizie particolari o sensibili**

Nel caso un elaborato consegnato alla scuola contenga dati personali o familiari particolari o sensibili, va custodito con cura in busta chiusa (su cui sarà annotato nome dell'interessato, descrizione del contenuto, data) e chiuso in posto sicuro. Al suo posto, insieme agli altri elaborati si metterà un foglio con l'annotazione del luogo di conservazione.

- **Procedura di Protezione Dati PP36: gestione degli elenchi degli alunni**

Anche gli elenchi contenenti soltanto dati anagrafici degli alunni godono di protezione da parte del D.Lgs 196/2003. Pertanto possono essere consegnati a terzi, soprattutto privati, esclusivamente per attività istituzionali della scuola. Va comunque previamente chiesta l'autorizzazione al Dirigente o al Responsabile.

5 - Trattamenti da parte dei membri di organi collegiali (anche esterni alla scuola)

*Queste Istruzioni vanno **applicate** dalla categoria: **membri di organi collegiali**.*
*Vanno **lette** per necessaria conoscenza dalle seguenti categorie: **Collaboratori del Dirigente**, **Assistenti Amministrativi** e **DGSA** in quanto di supporto, **Collaboratori Scolastici** in quanto di supporto*

- **Procedura di Protezione Dati PP37: gestione di documenti scolastici**

In generale qualunque documento scolastico che contenga dati personali di qualcun altro è sottoposto dal D.Lgs 196/2003 a una qualche forma di protezione, quindi va custodito in modo che nessun altro possa visionarlo, copiarlo o impadronirsene. Se non c'è motivo di detenerlo, va consegnato in segreteria per l'archiviazione.
L'obbligo è ancora più stringente se il dato è di tipo particolare, sensibile o giudiziario.
Chi avesse originale o copia di un tale documento deve custodirlo con cura dalla visione di terzi e riconsegnarlo alla segreteria appena non serve più. E' vietato conservarlo quando è cessato il motivo istituzionale per cui il dato è stato acquisito.

6 - Trattamenti da parte dei Collaboratori Scolastici

*Queste Istruzioni vanno **applicate** dalla categoria: **Collaboratori Scolastici** e **Personale Ausiliario**.*
*Vanno **lette** per necessaria conoscenza dalle seguenti categorie: **Collaboratori del Dirigente**, **Assistenti Amministrativi** e **DGSA** in quanto di supporto*

- **Procedura di Protezione Dati PP38: gestione di documenti scolastici**

In generale qualunque documento scolastico che contenga dati personali di qualcun altro è sottoposto dal D.Lgs 196/2003 a una qualche forma di protezione, quindi va custodito in modo che nessun altro possa visionarlo, copiarlo o impadronirsene. Se non c'è motivo di detenerlo, va consegnato in segreteria per l'archiviazione.
L'obbligo è ancora più stringente se il dato è di tipo particolare, sensibile o giudiziario.
Chi avesse originale o copia di un tale documento deve custodirlo con elevatissima cura e cautela dalla visione di terzi e riconsegnarlo alla segreteria appena non serve più.
Anche gli elenchi contenenti soltanto dati anagrafici degli alunni godono di protezione da parte del D.Lgs 196/2003. Pertanto possono essere consegnati a terzi, soprattutto privati, esclusivamente per attività istituzionali della scuola. Va comunque previamente chiesta l'autorizzazione al Dirigente perché potrebbe costituire atto illegittimo.
Pertanto qualsiasi registro, elaborato, elenco, certificato, e in generale documento scolastico che contiene dati personali di qualcuno va custodito con cautela, impedendo che altri ne prendano visione, lo copino o se ne impadroniscano.

- **Procedura di Protezione Dati PP39: trasporto di documenti scolastici**

I documenti ricevuti aperti vanno immediatamente consegnati alla segreteria, senza prenderne visione.
Nel caso di trasporto di documenti alla posta o ad altri destinatari o di ricezione di documenti destinati alla scuola, vanno trattati con cura, protetti da accesso di terzi, mai lasciati incustoditi, consegnati appena possibile alla segreteria o al legittimo destinatario.
Nel caso di documenti da consegnare internamente alla scuola vanno adottate analoghe cautele.

- **Procedura di Protezione Dati PP40: custodia**

Le ***stanze contenenti archivi*** e non presenziate devono essere mantenute *chiuse* e si deve intervenire immediatamente se un non-Incaricato vi accede.
Stanze contenenti archivi non posti in contenitori chiusi a chiave e in cui si conservano anche documenti sensibili o giudiziari sono ad accesso controllato, il che significa che la chiave è gestita dal DGSA o da un suo delegato "Custode delle chiavi".
La ***Presidenza*** e gli ***uffici*** in genere vanno *chiusi a chiave* quando non presenziati dal relativo personale.
E' fatto divieto assoluto a chiunque non ne abbia ricevuto esplicita autorizzazione di accendere o utilizzare i computer della segreteria o della presidenza o che comunque contengano dati personali. Si deve intervenire immediatamente se una persona non autorizzata tenta di farlo.
Fuori dall'orario di apertura della scuola non si deve far entrare nei locali citati alcun estraneo se non autorizzato.

- **Procedura di Protezione Dati PP41: partecipazione dei Collaboratori scolastici alle procedure della segreteria**

Questa procedura riguarda la partecipazione alle procedure già indicate per la segreteria, che richiedono il supporto consapevole e attento dei Collaboratori Scolastici.

Il Dirigente Scolastico
(prof. Ivano VACCARI)