Ministero dell'Istruzione, dell'Università e della Ricerca

UFFICIO SCOLASTICO REGIONALE PER LA CAMPANIA

Istituto Comprensivo Statale

Montesarchio 1° - Benevento

Procedure di protezione dati

Mansionario

Data creazione 1 SETTEMBRE 2017

Regole generali del Codice della Privacy DLgs 196/03

Istruzioni che vanno applicate da tutti gli Incaricati

Art. 1. 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. 2. Trattamenti con strumenti elettronici

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:

a) autenticazione informatica;

b) adozione di procedure di gestione delle credenziali di autenticazione;

c) utilizzazione di un sistema di autorizzazione;

d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli Incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;

e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;

f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;

g) tenuta di un aggiornato documento programmatico sulla sicurezza;

h) 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. 3. Trattamenti senza l'ausilio di strumenti elettronici

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.

2. Procedure per Trattamenti con supporto cartaceo

Istruzioni applicate a: Assistenti Amministrativi e DGSA, Collaboratori Scolastici per quanto di loro pertinenza.

A conoscenza di: Collaboratori del Dirigente, Collaboratori Scolastici in quanto di supporto alla Segreteria

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 per il trattamento.

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

- i documenti in ingresso devono essere utilizzati soltanto dagli Incaricati al trattamento dei dati o dal Responsabile;
- l'Incaricato deve verificare:
  - la corretta 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 alle finalità del trattamento, la completezza, la correttezza e l'aggiornamento dei dati;
- l'Incaricato deve valutare se è necessaria l'informativa (e se è necessaria la postilla per i dati sensibili e giudiziari di cui all'art. 22).

Informativa per la raccolta di dati

Dati comuni o particolari

Ogni raccolta di dati personali comuni o particolari deve essere accompagnata dalla sottoscrizione per attestazione della presa visione dell'apposita informativa di cui all'art. 13 che è fornita dal Titolare.

Ogni istanza rivolta alla scuola deve essere redatta su un modulo che in calce riporti per intero il testo dell'informativa, in modo che la firma dell'istanza stessa funga anche da attestazione della presa visione dell'informativa stessa. Pertanto non si accettano istanze su fogli bianchi. Tassativamente vanno utilizzati gli appositi moduli che hanno la parte superiore bianca e in calce riportano l'informativa. In casi eccezionali l'informativa può essere applicata all'originale, però è necessaria coincidenza di data e un chiaro riferimento al

documento a cui si riferisce.

Per quanto riguarda dipendenti, collaboratori, ecc. al momento dell'inizio del rapporto l'informativa deve prevedere anche le probabili comunicazioni di dati personali alle varie istanze del MIUR, alla Regione, al Tesoro, alla Ragioneria Provinciale dello Stato, all'INPS (se T.D.) o all'INPDAP, al Ministero Funzione Pubblica per l'anagrafe delle retribuzioni, alla scuola di provenienza e alla scuola a cui fossero trasferiti, ecc. .

Informativa da inserire <u>obbligatoriamente</u> in tutte le dichiarazioni sostitutive di certificazione e di atto notorio:

Ai sensi dell'art. 48 del D. P. R. n. 445 del 28 dicembre 2000 (Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa), è obbligatorio inserire l'informativa nella modulistica per la presentazione delle dichiarazioni sostitutive di certificazione e di atto notorio.

E' opportuno comunque inserire l'informativa in via generale in tutta la modulistica relativa alle istanze da presentare alla scuola. Si utilizzerà lo stesso testo dell'informativa di cui sopra.

<u>Dati sensibili o giudiziari</u>

Ogni raccolta di dati personali sensibili o giudiziari deve essere accompagnata dalla sottoscrizione per attestazione della presa visione dell'apposita informativa di cui all'art. 13, che è fornita dal Titolare ad inizio anno scolastico.

Tra i soggetti a cui i dati sensibili potranno essere comunicati va sempre indicata, sia per gli alunni che per i dipendenti, anche la scuola, ovviamente al momento sconosciuta, alla quale potrebbero trasferirsi.

Anche la scheda della registrazione assenze va autorizzata da apposita informativa, se le assenze per motivi di salute sono indicate con un codice che le renda riconoscibili.

Al momento dell'istituzione di ciascun Fascicolo Personale l'Interessato autorizza con l'informativa di cui sopra la trasmissione alla scuola in cui si dovesse trasferire e devono essere citati i trattamenti di certificati medici sia per giustificare l'assenza, sia per ottenere esoneri o benefici, sia a scopo di godere le coperture assicurative Inail o dell'eventuale assicurazione privata della scuola, sia per le comunicazioni di legge.

Nel caso sia raccolto un dato sensibile o giudiziario (ad esempio i certificati medici, i moduli che richiedono se l'Interessato ha riportato condanne oppure se è di sana e robusta costituzione, ecc.) si fa riferimento all'informativa.

Trattamento su richiesta dell'Interessato

Qualunque trattamento di dati su richiesta dell'Interessato, se presentato da terzi, deve essere tassativamente autorizzato con delega scritta. Ovviamente per gli alunni minorenni, il genitore o la persona esercente la patria potestà non ha bisogno di delega.

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, anche se non costituente documento definitivo, (appunti, stampe interrotte, stampe di prova, stampe elaborazioni temporanee ecc.) con le stesse cautele che sarebbero riservate alla versione definitiva (cfr. misure relative ai trattamenti cartacei e informatizzati).

Prima di consegnare o spedire documenti, verificare che esistano in atti le necessarie ed adeguate informative.

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).

Verifica della legittimità del trattamento in corso

Il Responsabile o l'Incaricato devono costantemente chiedersi se la fase dello specifico trattamento dati in corso rientra nel preciso ambito di responsabilità.

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

1. 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;
2. 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);
3. Ogni fase del trattamento rispetti le norme di legge e di regolamento;
4. In ogni fase del trattamento siano adottate le misure di sicurezza previste per la categoria alla quale il dato appartiene;
5. Se il dato è sensibile o giudiziario, siano rispettati i presupposti per avere la legittimazione a trattarlo;
6. In caso di comunicazione o diffusione, che il dato rientri nelle categorie autorizzate.

Documenti di Alunni e Personale alla conclusione del rapporto

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. Se trascorso un lasso ragionevole di tempo, l'interessato o un suo delegato non si presenterà a ritirarli, si avvierà una procedura di distruzione dei documenti con apposito verbale, ovviamente valutando prima se ci sono documenti che non sia opportuno eliminare (ad esempio, diplomi originali e simili).

In ogni caso qualunque fascicolo personale che transiti dall'archivio corrente a quello storico, dev'essere prima depurato di tutti dati personali non più necessari.

Trattamento di un documento 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.

Incaricati del trattamento di una pratica

I documenti contenenti dati personali di tipo sensibile, giudiziario, devono essere visti e conosciuti dal minor numero possibile di Incaricati. Le pratiche relative a tali documenti devono essere seguite nell'intero iter possibilmente da una sola persona (compresa la fase di protocollo), salvo diversa disposizione del Dirigente o del Responsabile.

Responsabilità dell'affidamento all'Incaricato

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. Non devono essere lasciati sui tavoli o comunque fuori dai contenitori documenti o fascicoli contenenti dati personali.

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 una stanza ad accesso riservato, almeno in quel momento, in modo che nessun altro possa sbirciarli o tanto meno trovarli momentaneamente abbandonati sul tavolo. Nei momenti di non utilizzo è necessario conservarli dentro un cassetto o un armadio chiuso a chiave, del quale soltanto l'Incaricato ha la chiave**.**

Custodia separata per dati relativi allo stato di salute

Per dati relativi allo stato di salute ed alle abitudini sessuali (omosessualità, reati di tipo sessuale, ecc.) c'è l'obbligo di **custodia separata** rispetto agli altri dati trattati per finalità che non richiedono il loro utilizzo.

Regole generali per la sicurezza degli archivi

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 terzi;
- 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 fornendogli la chiave o mettono a disposizione la chiave in modo che solo questi possono utilizzarla). E’ fondamentale assicurarsi che esista un numero definito di chiavi e che la chiave di riserva sia chiusa in luogo ben protetto. E’ stato nominato con atto formale un Incaricato “Responsabile delle chiavi” che deve controllare;
2) Ad alta sicurezza, ovviamente per dati sensibili o giudiziari, con accesso non solo selezionato, ma anche “controllato”: c’è una sola chiave disponibile e l’Incaricato che ne ha bisogno e che è autorizzato deve chiederla al “Responsabile delle chiavi”. Chi accedesse fuori orario di lavoro, deve annotarlo in apposito registro. Peraltro 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. Gli Incaricati che custodiscono dati personali su supporto cartaceo devono verificare che la dotazione di arredi (cassettiere, armadi ecc.) muniti di meccanismi di serratura adatta a garantire la sicurezza sia adeguata, altrimenti devono 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; la chiusura a chiave garantisce tanto la selezione del personale autorizzato ad accedere, quanto il controllo sugli accessi medesimi.

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, se appare agevole l'intrusione dall'esterno, muniti di sbarre. 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, anche se i documenti sono custoditi in contenitori chiusi a chiave, in quanto aumenta il livello di protezione dei dati stessi.

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 spazi dai quali possano essere gettati materiali o liquidi 5) nelle vicinanze devono essere presenti idonei dispositivi antincendio 6) è auspicabile la presenza di un sensore antincendio, anche autonomo.

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.

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 DGSA o dal Custode delle chiavi.

Archiviazione separata

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 dell'interessato, tipo di documento, data. Per i documenti contenenti dati particolarmente sensibili, invece del nome sulla busta si deve scrivere un codice e la data.

La corrispondenza tra codice e nome dell'interessato sarà riportata in un foglio o un registro, posto in una busta chiusa gestita dal Responsabile o dal Titolare, e posto in luogo sicurissimo e protetto.

La busta viene archiviata in uno degli Armadi cosiddetti "dei Dati Protetti" (permanentemente chiuso a chiave, ad accesso controllato, in una stanza normalmente chiusa a chiave quando non presenziata ed eventualmente protetta da antifurto).

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

Conservazione di registri e altri documenti non più utilizzati

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. L'eliminazione dei documenti avviene mediante la relativa Procedura di Protezione Dati.

Archiviazione nel fascicolo personale

I documenti non archiviati nell'Armadio di Protezione dati, 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, fino a fine anno scolastico, poi eliminati con la procedura di Protezione Dati. Il fascicolo personale è conservato nel relativo archivio corrente: in cassettiere metalliche chiuse a chiave negli orari non lavorativi e normalmente presidiate da almeno un Incaricato dei trattamenti (ovvero un dipendente assegnato alla segreteria), in una stanza in cui non sono ammessi di regola estranei, che viene chiusa a chiave al di fuori dell'orario lavorativo.

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 viene depurato dei documenti non più necessari, quindi archiviato nel corrispondente archivio storico, collocato in una stanza chiusa a chiave, ad accesso selezionato.

Scarto periodico dei documenti

Scarto periodico dei documenti contenenti dati personali di qualunque livello , ai sensi dell'art. 11 comma e del D.Lgs 196/03, 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 tutti gli archivi vengono passati al vaglio e vengono eliminati i documenti non più necessari, previa autorizzazione del Titolare del trattamento

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 taglia 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.

Appunti, bozze e copie superflue

Anche gli appunti, le bozze, le stampe intermedie, le fotocopie superflue costituiscono elemento di rischio, maggiorato quando trattasi di pratiche comprendenti anche documenti sensibili o giudiziari. Pertanto essi vanno distrutti con la prescritta procedura o , se necessario conservarli, archiviati insieme all'originale del documento sensibile o giudiziario.

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. A maggior ragione questo si applica se l'operazione di fotocopiatura avviene in una stanza ad accesso libero.

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.

Pulizia dei locali contenenti archivi

L'accesso di dipendenti o estranei per la pulizia dei locali contenenti archivi cartacei deve essere effettuata solo con i contenitori chiusi a chiave. Altrimenti le operazioni, anche se brevi, devono essere effettuate in presenza di un Incaricato della segreteria. Se vi sono contenuti dati sensibili e non sono chiudibili in contenitore, la pulizia deve essere effettuata esclusivamente alla presenza di un Incaricato del trattamento di tali dati.

Ingresso personale esterno per manutenzione

L'accesso di dipendenti o estranei per la manutenzione dei locali contenenti archivi cartacei o delle attrezzature in tali stanze contenute, deve essere effettuata solo con i contenitori chiusi a chiave. Altrimenti le operazioni devono essere effettuate in presenza di un Incaricato. 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.

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. Procedure per Trattamenti con strumenti elettronici

Istruzioni applicate a: Assistenti Amministrativi e DGSA, Collaboratori Scolastici per quanto di loro pertinenza

A conoscenza di: Collaboratori del Dirigente, Collaboratori Scolastici in quanto di supporto alla Segreteria

Sistema di autenticazione all'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 possono consistere in una di queste soluzioni:
   a) un codice per l'identificazione dell'Incaricato (user-id o username o 'nome utente') fisso e parzialmente riservato cui è associata una password segretissima modificabile;
   b) oppure in una tessera magnetica (come quella fornita dal MIUR per il computer intranet) in possesso e uso esclusivo dell'Incaricato, associata a un codice di identificazione dell'Incaricato (user-id o username) fisso e parzialmente riservato associata una password segretissima modificabile.
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) nonché la diligente custodia della tessera magnetica in possesso ed uso esclusivo dell'Incaricato.
5. La parola chiave, quando é prevista dal sistema di autenticazione, deve 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.

   Costituisce infrazione gravissima scrivere una password o una user-id su fogli di carta o quaderni, specialmente se in vicinanza del computer. E' vietato anche tenerla nel cassetto, benché chiuso a chiave. Se non si può memorizzarla, è consentito soltanto conservarla mascherata,ad esempio, premettendo e posponendo un certo numero di lettere o cifre.
6. Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri Incaricati, neppure in tempi diversi.
7. Le credenziali di autenticazione non utilizzate da almeno sei mesi vanno disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.

8. Le credenziali vanno disattivate anche in caso di perdita della qualità che consente all'Incaricato l'accesso ai dati personali.
9. Gli Incaricati non devono lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.
10. 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", che la riporrà in cassaforte o in altro armadio sicuro. Questa procedura è adottata per consentire al Titolare di assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'Incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, oppure nel caso che l'Incaricato "dimentichi" la password . Si evidenzia che il Codice sulla Privacy cita in merito: "*In tal caso la custodia delle copie delle credenziali é organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti Incaricati della loro custodia, i quali devono informare tempestivamente l'Incaricato dell'intervento effettuato*."
11. 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.

Sistema di autorizzazione

12. Quando per gli Incaricati sono individuati profili di autorizzazione di ambito diverso (per esempio per trattare dati sensibili o giudiziari) é utilizzato uno specifico sistema di autorizzazione.
13. I profili di autorizzazione, per ciascun Incaricato o per classi omogenee di Incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento. L'implementazione di questo sistema di autenticazione prevede che:

    Il Titolare o il Responsabile individuano quali profili di autorizzazione sono necessari per gli Incaricati che utilizzano il computer. In pratica stabiliscono quali computers 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 dell'assistenza 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 dell'assistenza dovrà provvedere anche a tradurre in pratica operativamente le altre indicazioni strategiche sulla gestione dei programmi e dei loro aggiornamenti, del back up, dell'antivirus, del firewall e dei sistemi di ripristino dati in caso di "disastro informatico".

Salvataggio dei dati (back-up)

Gli Incaricati sono tenuti a salvare i dati con frequenza almeno quindicinale. Pertanto procederanno al back up su disco fisso del server e su altro supporto informatico alla scadenza stabilita. Questi ultimi verranno riposti nell'armadio protetto di cui è Responsabile il DGSA e che deve restare sempre chiuso.

Cifratura dei file recanti dati idonei a rivelare lo stato di salute e la vita sessuale

Per i dati personali idonei a rivelare lo stato di salute e la vita sessuale, il file va salvato mediante il sistema di cifratura che viene fornito dal DGSA. Le parti di documento o archivio che riguardano questi dati vanno archiviate, se possibile, in un file separato e specifico, rispetto agli altri dati personali dell'interessato (e ,se possibile, in una directory separata).

Ciò viene fatto allo scopo che gli accessi agli dati dell'interessato non implichino anche la possibilità di vedere anche questi dati particolarmente protetti. Quando si trattano dati personali idonei a rivelare lo stato di salute o le abitudini sessuali o in generale dati particolarmente sensibili, nei limiti del possibile si deve farlo con una sessione priva di interruzioni o di abbandoni della postazione, in modo da rendere la visione dei dati su schermo il più breve possibile. Nel caso di interruzioni, si deve chiudere il file. Se altre persone, anche Incaricati, si avvicinano al computer di lavoro, devono essere invitati ad allontanarsi.

La parola chiave o simile utilizzata per la cifratura dev'essere nota soltanto all'Incaricato, che la scriverà su un foglio di carta con il nome e la collocazione del file e la password. Tale foglio sarà chiuso in busta sul cui esterno si scriverà il nome e la collocazione del file e quant'altro serve per l'identificazione. La busta sarà affidata al DGSA o al nominato "Custode delle Password" se nominato, che la riporrà in luogo sicurissimo.

Attenzione: non utilizzare il sistema di protezione con password di accesso fornita da certi programmi (es. a Word, Excel, ecc.) perché può indurre una falsa sicurezza. Sono diffusissimi programmi, anche freeware, per forzare con facilità tale protezione.

Programmi e dispositivi firewall

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 operatori molto esperti nell'utilizzare la connessione della scuola

a internet per introdursi nei computers durante il collegamento e copiare dati o manometterli; alcuni di loro sono definiti “hackers”).

Molto utile è l’aggiornamento periodico del Sistema Operativo, tramite internet, presso il sito del produttore, il quale identifica i “buchi” del sistema operativo che consentono l’accesso indesiderato dall’esterno e vi rimedia mettendo a disposizione una “pezza” (patch) che copre il buco. Da notare che le patches servono anche contro i virus e simili perché anch’essi utilizzano le falle del sistema.

La protezione da queste “intrusioni logiche” viene effettuata in due modi:

a) uno a bassa sicurezza, con un apposito programma denominato “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. Tale programma sarà acquistato dalla scuola e fornito agli Incaricati dal DGSA. Se necessario, si ricorrerà all’intervento di un tecnico esterno per l’installazione e la formazione degli Incaricati alle tecniche di aggiornamento e di utilizzo.

b) uno ad elevata sicurezza, mediante un apparecchio denominato “firewall, che si colloca fisicamente tra il modem e il computer. Esso è un tipo particolare di computer, fornito di un apposito software, che realizza le stesse cose di cui al punto precedente, ma in modo decisamente più efficace e affidabile. Il suo software va aggiornato con regolarità.

Programmi antivirus

Virus, worms e altri programmi pericolosi

I dati devono essere permanentemente protetti contro virus, worms, e altri programmi informatici che possono causare perdita di dati, malfunzionamenti, danni all’hardware, trasmissione all’esterno di files contenuti nel computer). Tali virus possono infettare il computers tramite l’uso di dischetti o l’accesso a certi siti internet o tramite la posta elettronica (in particolare i cosiddetti “allegati”). La protezione viene effettuata mediante l'utilizzo di un programma antivirus, acquistato dalla scuola e fornito agli Incaricati dal DGSA. Se necessario, si ricorrerà all’intervento di un tecnico esterno per l’installazione e la formazione degli Incaricati alle tecniche di aggiornamento e di utilizzo. Il programma antivirus deve essere aggiornato almeno ogni settimana. L’Incaricato è tenuto a verificare che queste condizioni siano attuate e 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.

Uso di supporti rimovibili

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 computers 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 (floppy disk e i CD) devono essere utilizzati esclusivamente per le copie di sicurezza (back-up) e subito devono essere riposti nel luogo sicuro indicato.

Cautele nel riutilizzo dei supporti rimovibili

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 (formattando il disco e verificando l'avvenuta operazione: non basta assolutamente cancellare i files)

Accesso di manutentori software o hardware

Se una delle misure minime di sicurezza elencate sono attuate tramite l'intervento di soggetti esterni alla propria struttura, 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.

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. Se dati sensibili o giudiziari non sono chiudibili in contenitore, la pulizia deve essere effettuata alla presenza di un Incaricato del trattamento di tali dati. Durante l'accesso per la pulizia tutti i computers contenenti dati sensibili o giudiziari devono essere spenti (o in modalità screen saver con password di ripristino) oppure deve presenziare un Incaricato del trattamento di tali dati.

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 dei locali o delle attrezzature contenute in tali stanze, deve essere effettuata solo con i contenitori chiusi a chiave. Se i dati sensibili o giudiziari non sono chiudibili in contenitore, l'intervento deve essere effettuata alla presenza di un

Incaricato del trattamento di tali dati. Durante l'accesso per l'intervento tutti i computers contenenti dati sensibili o giudiziari devono essere spenti oppure deve presenziare un Incaricato del trattamento di tali dati. Si noti che sottraendo un disco di back up, un malintenzionato può ricostruire gli archivi della scuola, violando dati personali.

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.

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 quest'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.

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 apre la busta chiusa riposta in luogo sicuro dov'è scritta la password. Poi la mette in una nuova busta chiusa;
4) 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.

Protezione dal furto di Notebook contenenti dati personali

Chi sottraesse un computer portatile avrebbe la possibilità di accedere ai dati personali eventualmente in esso contenuti. Considerata la facilità con cui possono essere sottratti, tali computer non devono essere utilizzati per dati sensibili o giudiziari. Vanno rigorosamente chiusi in armadio di sicurezza o cassaforte quando non utilizzati.

4. Trattamenti da parte dei docenti

Istruzioni applicate a: Docenti.

A conoscenza di: Collaboratori del Dirigente, Collaboratori Scolastici in quanto di supporto ai docenti

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: gli Incaricati devono 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, dev'essere mantenuto protetto da accessi non autorizzati e riconsegnato quanto prima al Dirigente o alla segreteria perché lo riponga in luogo sicuro.

Certificazioni mediche e informazioni sullo stato di salute degli 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 visionati solo se necessario e subito restituiti all'interessato affinché li consegni in segreteria. Questo vale in particolare per i certificati di esonero o limitazione presentati per educazione fisica; l'insegnante prenda nota dei limiti da osservare e faccia recapitare dall'interessato il certificato 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 grave shock anafilattico, asma grave con pericolo di soffocamento, diabete grave, epilessia, cardiopatie gravi, 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 che incide sulla didattica, 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 mettendoli in busta chiusa su cui sarà annotato nome dell'interessato, descrizione del contenuto, data e l'annotazione "*Da conservare separatamente in armadio sicuro*". Al suo posto, insieme agli altri elaborati si metterà un foglio con l'annotazione del luogo di conservazione.

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 e poi consegnato personalmente in segreteria mettendolo in busta chiusa su cui sarà annotato nome dell'interessato, descrizione del contenuto, data e l'annotazione "*Da conservare separatamente in armadio sicuro*". Al suo posto, insieme agli altri elaborati si metterà un foglio con l'annotazione del luogo di conservazione.

Gestione degli elenchi degli alunni

Anche gli elenchi contenenti soltanto dati anagrafici degli alunni godono di protezione da parte del D.Lgs. 196/03. 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.

Gestione di documenti scolastici

In generale qualunque documento scolastico che contenga dati personali di qualcun altro è sottoposto dal D.Lgs. 196/03 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.

5. Trattamenti da parte dei membri di organi collegiali

Istruzioni applicate a: membri di organi collegiali.

A conoscenza di: Collab. del Dirigente, Assistenti Amm.vi, DGSA e Collaboratori Scolastici in quanto di supporto

(anche esterni alla scuola)

Gestione di documenti scolastici

In generale qualunque documento scolastico che contenga dati personali di qualcun altro è sottoposto dal D.Lgs. 196/03 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.

Anche gli elenchi contenenti soltanto dati anagrafici degli alunni godono di protezione da parte del D.Lgs. 196/03. 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.

6. Trattamenti da parte dei Collaboratori Scolastici e Pers. Ausiliario

Istruzioni applicate a: Collaboratori Scolastici e Personale Ausiliario.

A conoscenza di: Collaboratori del Dirigente, Assistenti Amministrativi e DGSA in quanto di supporto

Gestione di documenti scolastici

In generale qualunque documento scolastico che contenga dati personali di qualcun altro è sottoposto dal D.Lgs. 196/03 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. 196/03. Pertanto possono essere consegnati a terzi, soprattutto privati, esclusivamente per attività istituzionali della scuola. Va comunque previamente chiesta l'autorizzazione al Dirigente per la verifica della legittimità dell'atto.

Pertanto qualsiasi registro, elaborato, elenco, libretto personale, 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.

Trasporto di documenti scolastici

I documenti ricevuti aperti vanno immediatamente consegnati alla segreteria, senza prenderne visione. Se c'è il sospetto che si tratti di certificati medici, certificazioni relativi ai redditi, ecc. si deve offrire all'interessato una busta chiusa affinché ve li inseriscano.

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.

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". Chi dovesse accedere per manutenzioni o pulizie, deve farlo chiedendone il

permesso, limitando al massimo il tempo di permanenza ed evitando di lasciare la stanza incustodita o di farvi accedere altri. Se ritenuto necessario dal DGSA deve presenziare un addetto alla segreteria.

La Presidenza, la segreteria 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 computers della segreteria o della presidenza o che comunque contengano dati personali. Si deve intervenire immediatamente se una persona non autorizzata tenta di farlo.

Se esterni per motivi di manutenzione devono entrare nelle stanze citate o negli archivi per i quali è prevista la chiusura a chiave, vanno seguiti a vista; se questo è impossibile, vanno invitati a tornare in altro momento, a meno che non sia in atto un'emergenza urgente che richiede il loro intervento.

Fuori dall'orario di apertura della scuola non si deve far entrare nei locali citati alcun estraneo.

Partecipazione alle procedure della segreteria

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

Il Titolare del Trattamento dei dati/ Dirigente scolastica

Maria Rosaria Damiano