Misure di protezione di dati personali

A tutte le categorie di incaricati

REGOLE GENERALI DEL CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI D.lgs 196/2003

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: 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; 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. 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.

Istruzioni per: DSGA, Assistenti Amm.vi, Collaboratori del D.S.

TRATTAMENTO DATI CARTACEI

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: o i documenti in ingresso devono essere utilizzati soltanto da chi sia Incaricato al trattamento dei dati che contengono o dal Responsabile; o 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; o l'Incaricato deve valutare se è necessaria l'informativa
Informativa per la raccolta di dati comuni o particolari	Ogni raccolta di dati personali comuni o particolari dev'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 dev'essere redatta su un modulo che in calce riporti per intero il testo dell'informativa di cui al punto precedente, in modo che la firma dell'istanza stessa funga anche da attestazione della presa visione dell'informativa stessa. In alcuni casi 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, commissari d'esame 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. E' opportuno inserire l'informativa in via generale in tutta la modulistica relativa alle istanze da presentare alla scuola.
Informativa per la raccolta di dati sensibili o giudiziari	Ogni raccolta di dati personali **sensibili o giudiziari** dev'essere accompagnata dalla sottoscrizione per attestazione della presa visione dell'apposita informativa di cui all'art. 13, che è fornita dal Titolare. Al momento dell'istituzione di ciascun Fascicolo Personale l'Interessato deve autorizzarlo con apposita informativa che consenta anche di mandarlo 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' assicurazione privata della scuola, sia per le comunicazioni di legge alla Questura e all'Inail. 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.) va utilizzata l'apposita informativa,
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 ad 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, stampe elaborazioni temporanee ecc.) con le stesse cautele che sarebbero riservate alla versione definitiva (v. misure relative ai trattamenti cartacei e informatizzati). Prima di consegnare o spedire documenti, verificare che esistano in atti le necessarie, 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	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)**. 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
Quando un dipendente o un alunno lascia la scuola	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. Se passato 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 verbalino, 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.
Classificazione immediata di ogni documento	Non appena qualsiasi Incaricato si accorge che un documento contiene dati personali di livello superiore a "comune" o "anonimo" , deve scrivere in matita sull'angolo destro superiore del foglio la sigla descrivente il tipo di dato : "**P**" = dato particolare, "S"=dato sensibile, "**G**"=dato giudiziario, seguita da "**b**" se si tratta di dato che per la sua natura rivela un'informazione modesta e poco pericolosa per l'interessato se conosciuta da estranei (es. certificato medico generico privo di diagnosi e di qualsiasi riferimento alla malattia o infortunio che lo ha generato), "**a**" per tutti gli altri casi. Nel dubbio, va scelta la lettera "**a**".
Trattamento appena viene ricevuto un documento	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
Limitare il numero di incaricati che trattano la pratica	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. 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
Affidamento all'incaricato sotto la sua responsabilità	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 chiusa, 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 utilizzazione di conservarli dentro un cassetto o un armadio chiuso a chiave, del quale soltanto l'Incaricato ha la chiave.
Custodia separata dei dati relativi alla 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 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). 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". 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. 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, se appare agevole l'intrusione dall'esterno, muniti di sbarre. In tal caso il personale diverso dagli Incaricati del trattamento che vi accede i 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 dev'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. 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) nelle vicinanze devono essere presenti idonei dispositivi antincendio 6) è auspicabile la presenza di un sensore antincendio, anche autonomo. 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
Archiviazione separata	I documenti contenenti dati sensibili, giudiziari o particolari <u>ad alto livello di delicatezza</u> vanno di norma chiusi in busta di carta, su cui è riportato nome dell'interessato, tipo di documento, data attuale e la scadenza per la eliminazione (se non conoscibile, mettere una data presunta seguita da un punto interrogativo).

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.
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 descritta di seguito. 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 al 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 196/2003, 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 tutti gli archivi vengono passati al vaglio e vengono eliminati i documenti non più necessari.
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)
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.
Cautela 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. A maggior ragione questo si applica se l'operazione di fotocopiatura avviene in una stanza ad accesso libero.
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 contenitori chiusi. 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
Ingresso di persone esterne per pulizia e/o manutenzioni dei locali contenenti archivi	L'accesso di dipendenti o estranei per la pulizia dei locali contenenti archivi cartacei dev'essere effettuata solo con i contenitori chiusi a chiave. Altrimenti le operazioni, peraltro brevi, devono essere effettuate in presenza di un Incaricato della segreteria. Se vi sono contenuti dati sensibili non chiudibili in contenitore, la pulizia deve essere effettuata 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

TRATTAMENTO DATI CON STRUMENTI ELETTRONICI

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 consistono in un codice per l'identificazione dell'Incaricato (user-id o username o 'nome utente') fisso e parzialmente riservato (è noto al gestore del sistema, perché deve assegnarlo ed è visibile ai manutentori software), cui è associata una password segretissima variabile che abbia le seguenti caratteristiche: • Originale • Composta da otto caratteri di cui almeno 1 sia un numero • Che non sia facilmente intuibile (evitando il proprio nome, il nome di congiunti, la data di nascita o riferimenti facilmente ricostruibili) 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 o parola chiave) 5. La parola chiave dev'essere modificata da ciascun Incaricato almeno ogni tre mesi. **Costituisce infrazione disciplinare gravissima scrivere una password o una user-id su fogli di carta o quaderni, tanto peggio se in vicinanza del computer. E' vietato anche tenerla nel cassetto, benché chiuso a chiave.** 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 come "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 ricorda che il Codice dice : "*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.*" **Sistema di autorizzazione** 11. 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. 12. 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'Amministratore di sistema o un tecnico dovrà costruire 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" (disaster recovery=recupero del disastro).
salvataggio dei dati (back-up)	Gli Incaricati sono tenuti a salvare i dati con frequenza almeno settimanale (lo dice il Codice). Pertanto procederanno al back-up in base alle disposizioni impartite, che verranno riposti nell'armadio protetto di cui è Responsabile il DGSA e che deve restare sempre chiuso. Si ricorda che il Codice prescrive: "*Devono essere adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni." Pertanto le copie di sicurezza devono essere aggiornate settimanalmente*.

Ulteriori misure in caso di trattamento di dati sensibili o giudiziari : Programmi firewall, 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 frequente del Sistema Operativo, tramite internet, gratuitamente presso il sito del produttore di tale software, 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, quindi bisogna aggiornare spesso il software. 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 ad elevata sicurezza, mediante un server con funzioni di "Firewall, che si colloca fisicamente tra il router e il computer.
Ulteriori misure in caso di trattamento di dati sensibili o giudiziari : Programmi antivirus	**Virus** I dati sono 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, installato su ogni PC. Il programma antivirus si aggiorna automaticamente ad ogni connessione visto che ogni giorno nascono nuovi virus). 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 dei supporti rimovibili	I floppy disk e i CD non devono essere utilizzati 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. I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati devono essere distrutti o resi inutilizzabili.
accesso di manutentori software o hardware	Sono state autorizzate, mediante specifico incarico, persone esterne alla scuola per la manutenzione dell'hardware o del software.
ingresso di persone esterne per manutenzione locali o impianti o attrezzature o pulizia dei locali	L'accesso di dipendenti o estranei per la pulizia dei locali contenenti dischi di back-up dev'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 salvaschermo con password di ripristino) oppure deve presenziare un Incaricato del trattamento di tali dati
procedure ad ogni variazione degli Incaricati	Se entra in servizio un Incaricato che ha accesso alle risorse informatiche l'Amministratore di sistema 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, l'Amministratore di sistema deve provvedere a fare in modo che sia annullato il suo sistema di credenziali.
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. 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.

Ogni trattamento di dati sensibili e/o giudiziari dovrà essere conforme a quanto previsto dal D.M. n.305 del 7/12/06 e come descritto nelle schede applicative che sono state oggetto di specifica formazione e messe a disposizione di tutto il personale di segreteria.

Istruzioni per la componente Docenti

Trattamento da parte dei docenti

registri	I registri delle programmazioni e dei verbali di intersezione e interclasse devono essere sempre custoditi in modo sicuro. Il registro dei 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 attività motorie; 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, epilessia, cardiopatie 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 DGSA 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 contenitori chiusi 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 196/2003. 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.
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

Ogni trattamento di dati sensibili e/o giudiziari dovrà essere conforme a quanto previsto dal D.M. n.305 del 7/12/06 e come descritto nelle schede applicative che sono state oggetto di specifica formazione e messe a disposizione di tutto il personale di segreteria.

Istruzioni per la componente genitori degli organi collegiali

Trattamento dei dati da parte di membri degli organi collegiali

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. 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.

Istruzioni per la componente Collaboratori Scolastici

Trattamento dei dati da parte della componente Collaboratori Scolastici

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. 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.
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; inoltre, 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 computer 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. In questo caso informare il/i Collaboratori delle procedure di Segreteria