# Trattamenti dei dati personali su supporto cartaceo e/o informatico

*Queste Istruzioni vanno applicate dalla categoria: Docenti, Assistenti Amministrativi e DSGA, Assistenti Tecnici, Collaboratori Scolastici per quanto di loro pertinenza.*

## □ Procedura di Protezione Dati : **documenti in ingresso**

Per "documenti in ingresso", si intendono i documenti o i supporti contenenti dati personali acquisiti dalla scuola ai
fini di un loro impiego in trattamento.
relativamente al trattamento dei documenti in ingresso , è necessario adottare le cautele seguenti:

- i documenti in ingresso devono essere utilizzati soltanto da chi sia Incaricato al trattamento dei dati che contengono o dal Responsabile;
- l'Incaricato deve verificare:

- la provenienza dei documenti;
- che tali documenti siano effettivamente necessari al trattamento in questione;
- la tipologia dei dati contenuti (comuni, sensibili, , giudiziari o altri dati particolari), al fine di individuare le modalità legittime ed idonee per il trattamento e le misure di sicurezza da attuare;
- l'osservanza del principio di pertinenza e non eccedenza rispetto o alle finalità del trattamento, la completezza,
la correttezza e l'aggiornamento dei dati;

- 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, in tal caso compilandola).

## □ Procedura di Protezione Dati: **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. 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, 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.
**Informativa da inserire obbligatoriamente 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.

## □ Procedura di Protezione Dati : **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., diversa da quella per dati comuni perché richiede anche un completamento da parte dell'Incaricato. Infatti quest'ultimo deve indicare per quale precisa finalità serve il dato, citando tassativamente la legge o la disposizione a cui si riferisce la finalità dell'istanza, e indicando a chi il dato sarà comunicato (o potrebbe essere comunicato) o se il dato sarà diffuso.
Per quanto riguarda i certificati medici e le relazioni mediche, va graffettata ad essi l'informativa, compilata come sopra.
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 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,

## □ Procedura di Protezione Dati : **firma l'Interessato o c'è sua delega scritta**

Qualunque trattamento di dati su richiesta dell'Interessato, se presentato da terzi dev'essere tassativamente autorizzato da delega. Ovviamente per gli alunni minorenni, il genitore o la persona esercente la patria potestà non ha bisogno di delega. Per gli alunni maggiorenni anche il genitore ha bisogno della delega.
La delega va allegata all'informativa o all'istanza o alla ricevuta.

## □ Procedura di Protezione Dati : **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, , ancorchè non costituente documento definitivo, (appunti, stampe interrotte, stampe di prova, stampe elaborazioni temporanee ecc.) con le stesse cautele che sarebbero riservate alla a 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).

## □ Procedura di Protezione Dati : **verifica della legittimità del trattamento in corso**

Di fronte a qualsiasi nuovo trattamento di dati, il Responsabile del trattamento stesso e l'Incaricato devono chiedersi se rientra nel preciso recinto di legittimità, delimitato dai seguenti paletti:
Il trattamento sia connesso con **l'esercizio delle funzioni istituzionali** (principio di **pertinenza)** e che esse non siano perseguibili attraverso il trattamento di dati anonimi.
**1**.Le modalità del trattamento siano tali da determinare il minimo sacrificio possibile del diritto alla riservatezza dell'Interessato (principio di **non eccedenza:** è illegittimo chiedere un dato in più di quello che è strettamente necessario).
**2.**Ogni fase del trattamento rispetti **le norme di legge e di regolamento.**
**3.** In ogni fase del trattamento siano adottate le **misure di sicurezza previste per la categoria alla quale il dato appartiene**
**4**.Se il dato è sensibile o giudiziario, siano rispettati i presupposti per avere la legittimazione a trattarlo
**5**. In caso di comunicazione o diffusione, che il dato rientri nelle categorie autorizzate.

## □ Procedura di Protezione Dati : **quando un alunno o un dipendente ci lascia definitivamente.**

Gli vanno consegnati tutti i documenti contenenti dati personali che la scuola non sia obbligata a conservare.
Nel caso non fosse possibile trattare direttamente con l'Interessato, si deve mandare un avviso per il ritiro.
Nel frattempo i materiali da consegnare vanno posti in busta chiusa. Al ritiro va fatta firmare una ricevuta. Se passato un lasso ragionevole di tempo, l'interessato 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.

## □ Procedura di Protezione Dati : **classificazione immediata di ogni documento/ protocollo**

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".

## □ Procedura di Protezione Dati : **trattamento appena un documento viene ricevuto**

L'Incaricato che riceve "brevi manu" allo sportello o in qualsiasi altro punto della scuola documenti contenenti dati personali di tipo sensibile, giudiziario o particolare ad alto livello di delicatezza ancora non collocati in busta chiusa, deve immediatamente metterli in busta chiusa e inserirli nella posta in arrivo per il Dirigente Scolastico.

## □ Procedura di Protezione Dati : **circoscrivere al massimo il numero di Incaricati che trattano una 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.

## □ Procedura di Protezione Dati : **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.

## □ Procedura di Protezione Dati : custodia **separata per i 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.

## □ Procedura di Protezione Dati : **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". Chi accedesse fuori orario di lavoro, deve annotarlo in apposito registro. Riteniamo che la scuola non abbia necessità di accedere fuori orario, quindi non c'è ragione che esista tale 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.
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 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) Non lasciare pertugi di 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.
**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.
**Ciusura a chiave dei contenitori metallici:**
Gli armadi e contenitori che ospitano archivi vanno chiusi a chiave alla fine della giornata lavorativa e le chiavi vanno messe in luogo sicuro indicato dal DGSA O DAL Custode delle chiavi.

## □ Procedura di Protezione Dati **: 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 attuale e la scadenza per la eliminazione (se non conoscibile, mettere una data presunta seguita da un punto interrogativo). Per i documenti contenenti dati particolarmente sensibili, invece del nome sulla busta si deve scrivere un codice, la data attuale e la scadenza per la eliminazione.
La corrispondenza tra codice e nome dell'interessato sarà riportata in un foglio o un quaderno, 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[e 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.

## □ Procedura di Protezione Dati **: 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. L'eliminazione dei documenti avviene mediante la Procedura di Protezione Dati

## □ 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
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.

### ☐ Procedura di Protezione Dati : **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.

### ☐ Procedura di Protezione Dati : **scarto periodico dei documenti**

Scarto periodico dei documenti contenenti dati personali di qualunque livello , ai sensi dell'art. 11 comma e del D.Lgs196/2003, 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, utilizzando la Procedura di Protezione

### ☐ Procedura di Protezione Dati : **distruzione dei documenti**

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

### ☐ Procedura di Protezione Dati : **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.

### ☐ Procedura di Protezione Dati : **cautele nella fase di fotocopiatura**

Quando documenti contenenti dati personali di tipo sensibile, giudiziario o particolare ad alto livello di delicatezza devono essere fotocopiati, hanno la precedenza su tutti gli altri e devono essere adottate opportune cautele affinché nessun altro ne possa prendere visione. Tranne impossibilità tecnica, l'operazione di fotocopiatura deve essere effettuata dall'Incaricato che tratta la pratica. L'Incaricato deve fare in modo che il documento non venga lasciato in giacenza vicino alla fotocopiatrice né prima né dopo la fotocopiatura. A maggior ragione questo si applica se l'operazione di fotocopiatura avviene in una stanza ad accesso libero.

### ☐ Procedura di Protezione Dati : **la movimentazione da parte di terzi**

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

### ☐ Procedura di Protezione Dati : **pulizia 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 sono chiudibili in contenitore, la pulizia deve essere effettuata esclusivamente alla presenza di un Incaricato del trattamento di tali dati.

### ☐ Procedura di Protezione Dati : **ingresso di persone esterne per manutenzione**

L'accesso di dipendenti o estranei per la manutenzione dei locali contenenti archivi cartacei o delle attrezzature in talistanze contenute, dev'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.

### □ Procedura di Protezione 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 - Trattamenti con strumenti elettronici

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

### □ Procedura di Protezione Dati : 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 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 (è noto al gestore del sistema, perché deve assegnarlo ed è visibile ai manutentori software), cui è associata una password segretissima variabile;
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 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.
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 ) nonché la diligente custodia della tessera magnetica in possesso ed uso esclusivo dell'Incaricato (se esiste)
5. La parola chiave, quando é prevista dal sistema di autenticazione, dev'essere composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito. Essa non deve contenere riferimenti agevolmente riconducibili all'Incaricato (nomi o iniziali proprie o di parenti, date di nascita, e simili).
La parola chiave dev'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 dev'essere modificata almeno ogni tre mesi.
**Costituisce infrazione disciplinare gravissima scrivere una password o una user-id su fogli di carta o quaderni, tento peggio se in vicinanza del computer. E' vietato anche tenerla nel cassetto, benché chiuso a chiave. Se non si può memorizzarla, è consentito soltanto conservarla in un foglietto dentro il portafoglio, meglio se mascherata 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" (se nominato), 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."

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.

**Costituisce infrazione disciplinare gravissima scrivere una password o una user-id su fogli di carta o quaderni, tento peggio se in vicinanza del computer. E' vietato anche tenerla nel cassetto, benché chiuso a chiave. Se non si può memorizzarla, è consentito soltanto conservarla in un foglietto dentro il portafoglio, meglio se mascherata premettendo e posponendo un certo numero di lettere o cifre.**

**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 si fa in questo modo:

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 dovrà tradurre in pratica queste direttive, costruendo i necessari profili di autorizzazione differenziati per ciascun utilizzatore, al quale sarà consegnata la corrispondente credenziale di autenticazione ( più d'una se necessario).

L'Amministratore di sistema o un tecnico dovrà provvedere anche a tradurre in pratica operativamente le altre indicazioni strategiche sulla gestione dei programmi e dei loro aggiornamenti, del backup, dell'antivirus, del firewall (protezione dagli accessi tramite internet) e dei sistemi di ripristino dati in caso di "disastro informatico" (disaster recovery=recupero del disastro). Nel DPSS questi problemi dovranno essere sviscerati e indicate le soluzioni adottate(rinviamo a quella sede i chiarimenti ulteriori).

## □ Procedura di Protezione Dati : 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 su floppy disk , che verranno riposti nell'armadio protetto di cui è Responsabile il DGSA e che deve restare sempre chiuso. *[naturalmente se il sistema di back-up è diverso, indicarlo. Per esempio: su CD, oppure su dispositivi appositi di back-up oppure su altro computer della rete , ma in questo caso va garantita l'impossibilità di accesso a chi non ha il sistema di credenziali previsto]*

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.

Resta aperta la questione se il Codice obbliga o no anche le piccole strutture come le scuole a dotarsi di un sistema di back-up automatico e di "disaster recovery " (= recupero di un disastro) che oltre a salvare i dati, memorizza anche tutte le configurazioni del sistema ed è in grado di farlo ripartire. Successive istruzioni verranno date se e quando sarà attivo un apparato del genere.

## □ Procedura di Protezione Dati : 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 gratuiti, per forzare con facilità tale protezione.

## □ Procedura di Protezione Dati - 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. Poiché le falle dei sistemi windows sono moltissime, le patches da caricare sono altrettante, 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 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. Non è ben chiaro se quando la scuola sarà costretta dalle disposizioni per la sicurezza dei dati del D.Lgs 196/2003 ad acquistarne uno: In tal caso il programma "firewall" , di cui al punto precedente, diventa inutile.

## □ Procedura di Protezione Dati - Ulteriori misure in caso di trattamento di dati sensibili o giudiziari : Programmi antivirus

**Virus, worms (vermi) e altri programmi maligni**

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, che 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. Il programma antivirus deve essere aggiornato almeno ogni settimana [la norma prevede almeno 6 mesi, ma è sicuramente insufficiente, 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.

## □ Procedura di Protezione Dati : uso dei 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.

## □ Procedura di Protezione Dati : 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 (= riformattando il disco e verificando l'avvenuta riformattazione; non basta assolutamente cancellare i files !)

### □ Procedura di Protezione Dati – **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.

### □ Procedura di Protezione Dati : **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.

### □ Procedura di Protezione 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 in tali stanze contenute, dev'essere effettuata solo con i contenitori chiusi a chiave. Se 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.

### □ Procedura di Protezione Dati : **procedure ad ogni variazione degli Incaricati**

Se entra in servizio un Incaricato che ha accesso alle risorse informatiche il Responsabile o, in sua mancanza, il DGSA 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 o, in sua mancanza, il DGSA deve provvedere a fare in modo che sia annullato il suo sistema di credenziali.

### □ Procedura di Protezione Dati: **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.

### □ Procedura di Protezione Dati : **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 ( il DGSA ) 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.

### □ Procedura di Protezione Dati : **protezione dal furto di computers portatili 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 computers non devono essere utilizzati per dati sensibili o giudiziari. Vanno rigorosamente chiusi in armadio di sicurezza o cassaforte quando non utilizzati.