I S T I T U T O C O M P R E N S I V O '*G. MARCONI*'
di Castelfranco Emilia - Mo
Via Guglielmo Marconi, 1
Tel 059 926254 - fax 059 926148 email: MOIC825001@istruzione.it

Prot. n. **allegato 9**

Manuale per la Gestione in Sicurezza dei dati ad uso degli incaricati
Sintesi

D. Lgs. 196/2003
"Codice in materia di protezione dei dati personali" – *cd. "Privacy".*

Titolare del Trattamento Prof. Vilma Baraccani
Responsabile del Trattamento Massimo Caridi
Incaricati: assistenti amministrativi, docenti, collaboratori scolastici.

Introduzione

Questo documento fornisce agli incaricati del trattamento una panoramica sulle responsabilità loro spettanti rispetto alla gestione ed allo sviluppo della sicurezza della gestione del dato personale cui possono accedere, sia esso relativo a dipendenti che a clienti, fornitori, consulenti, ecc.

1 Alcune definizioni

Trattamento: qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, modifica, selezione, estrazione, raffronto, utilizzo, interconnessione, blocco comunicazione, diffusione, cancellazione e distribuzione dati;
Dati personali: qualunque informazione relativa a persona fisica, persona giuridica, ente o associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;
Dati identificativi: i dati personali che permettono l'identificazione diretta dell'interessato
Dati sensibili: i dati personali idonei a rilevare l'origine razziale ed etnica, le convinzioni religiose o filosofiche, le opinioni politiche, l'adesione a partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico, sindacale nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.
Dati giudiziari: i dati personali idonei a rivelare provvedimenti giudiziari
Titolare: persona fisica, giuridica, pubblica amministrazione e qualsiasi altro ente, cui competono le decisioni in ordine alle finalità, modalità del trattamento dei dati personali ed agli strumenti utilizzati ivi compreso il profilo della sicurezza.
Responsabile: persona fisica o giuridica, pubblica amministrazione e qualsiasi altro ente, associazione o organismo preposti dal titolare del trattamento di dati personali;
Incaricati: persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;
Interessato: persona fisica o giuridica, ente o associazione cui si riferiscono i dati personali;

2 Il D. Lgs 196/2003

Diritto di accesso ai dati

1. L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano anche non ancora registrati e la loro comunicazione in forma intelligibile.
2. L'interessato ha diritto di ottenere l'indicazione:
   a) dell'**origine** dei dati personali;
   b) delle **finalità** e delle **modalità** di trattamento;
   c) della logica applicata nel trattamento effettuato con l'ausilio di strumenti elettronici;
   d) degli estremi identificativi del **titolare**, dei **responsabili** e del **rappresentante** designato;
   e) dei soggetti o delle categorie ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato
3. L'interessato ha diritto di ottenere:
   a) aggiornamento, rettifica ovvero quando vi è interesse ad integrazione;
   b) cancellazione, trasformazione in forma anonima o blocco dei dati trattati in violazione di legge, compresi quelli di cui è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
   c) attestazione che le suddette operazioni sono state portate a conoscenza anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.
4. L'interessato ha diritto di opporsi:
   a) Per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;
   b) Al trattamento dei dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

Diritto al riscontro

1. A garanzia dell'effettivo esercizio dei diritti di cui all'art. 7, il titolare è tenuto ad adottare misure che:

Prot. n. **allegato 9**

a) agevolino l'accesso ai dati all'interessato anche con appositi programmi;
b) semplifichino modalità e riducano tempi per il riscontro da parte del richiedente.

2. Estrazione dati da responsabile o incaricato e comunicati anche oralmente a richiedente o offerti in visione mediante strumenti elettronici (se comprensione dati è agevole); su richiesta, obbligo trasposizione dati su supporto cartaceo o informatico, ovvero trasmissione per via telematica.
3. Il riscontro ha come oggetto TUTTI i dati personali del richiedente.
4. Se l'estrazione è difficoltosa, è sufficiente l'esibizione o la consegna di copia degli atti.
5. Non può riguardare dati personali relativi a terzi salvo connessione con dati interessato.
6. Obbligo di comunicazione con grafia comprensibile e se attraverso codici, obbligo fornitura chiavi di lettura idonee.
7. Se i dati sono inesistenti, il titolare ha diritto ad un contributo per i costi sostenuti.

3 Struttura organizzativa aziendale per la gestione della sicurezza dei dati personali

Titolare del Trattamento	D.S. Prof.ssa Vilma Baraccani	Ha la competenza e la responsabilità di decidere in merito alle finalità ed alle modalità di trattamento dei dati, nonchè alle misure di sicurezza da adottare.
Responsabile del Trattamento	DSGA Massimo Caridi	Persona preposta dal Titolare a: 1. individuare e nominare per iscritto gli incaricati del trattamento, insegnando loro, ancora per iscritto, le idonee istruzioni; 2. vigilare sul rispetto delle istruzioni impartite agli incaricati; 3. adottare e rispettare le misure di sicurezza indicate dal titolare del trattamento; 4. vigilare sul rispetto di dette misure di sicurezza da parte degli incaricati; 5. evadere tempestivamente tutte le richieste e gli eventuali reclami degli interessati; 6. evadere tempestivamente le richieste di informazioni da parte dell'autorità garante; 7. interagire con i soggetti incaricati di eventuali verifiche, controlli o ispezioni; 8. comunicare immediatamente al titolare gli del trattamento degli stessi eventuali nuovi trattamenti da intraprendere nel proprio settore di competenza, provvedendo alle formalità di legge; 9. distruggere i dati personali in caso di cessazione del trattamento degli stessi

Prot. n. **allegato 9**

Incaricato del Trattamento	Docenti Assistenti amministrativi Collaboratori scolastici	Persona che ha accesso a dati personali e come tale deve: 1. trattare tutti i dati personali di cui vengono a conoscenza nell'ambito dello svolgimento delle funzioni in modo lecito e secondo correttezza; 2. effettuare la raccolta, l'elaborazione, la registrazione di dati personali esclusivamente per lo svolgimento delle proprie mansioni; 3. accedere unicamente alle banche dati come indicate dai superiori; 4. aggiornare trimestralmente tutte le banche dati cui hanno accesso; 5. evitare di creare banche dati nuove senza espressa autorizzazione del titolare o del responsabile incaricato; 6. mantenere assoluto rispetto sui dati personali di cui vengono a conoscenza nell'esercizio delle loro funzioni; 7. evitare di asportare supporti informatici o cartacei contenenti dati personali di terzi senza autorizzazione del titolare.

4 Doveri dell'Incaricato

L'incaricato dovrà rispettare le istruzioni impartite dal Titolare o dal Responsabile.
In particolare dovrà:

- procedere alla raccolta di dati personali, anche mediante l'approvazione di appositi moduli di raccolta;
- consegnare agli interessati, al momento della raccolta dei dati, il modulo contenente 'informativa, salvo che l'informativa medesima sia stata fornita direttamente dal titolare o dal responsabile;
- raccogliere, sempre al momento della raccolta dei dati, il consenso espresso, documentato per iscritto, degli interessati ai trattamenti previsti, salvo che a ciò abbiano provveduto direttamente il titolare o il responsabile, e salvo i casi di esonero previsti dalla stessa legge;
- trattare i dati personali in modo lecito e secondo correttezza, nella misura necessaria e sufficiente alle finalità proprie della banca dati nella quale vengono inseriti;
- verificare, ove possibile, che siano esatti e provvedere, se necessario, al loro aggiornamento;
- verificare che siano pertinenti, completi e non eccedenti le finalità per le quali sono stati raccolti o successivamente trattati, secondo le indicazioni ricevute dal Titolare o dal Responsabile del Trattamento;
- adottare, nel trattamento dei dati, tutte le misure di sicurezza che siano indicate, oggi o in futuro, dal titolare o dal responsabile, in particolare dovrà quanto di seguito precisato:
  - per le banche dati informatiche, utilizzare sempre il proprio codice di accesso personale, evitando di operare su terminali altrui e/o di lasciare aperto il sistema operativo con la propria password inserita in caso di allontanamento anche temporaneo dal posto di lavoro, al fine di evitare trattamenti non autorizzati e di consentire sempre l'individuazione dell'autore del trattamento;
  - trattare i soli dati la cui conoscenza sia necessaria e sufficiente per lo svolgimento delle operazioni da effettuare;
  - conservare i supporti informatici e/o cartacei contenenti i dati personali in modo da evitare che detti documenti siano accessibili a persone non autorizzate al trattamento dei dati medesimi;
  - con specifico riferimento agli atti e documenti cartacei contenenti dati personali ed alle loro copie, restituire gli stessi al termine delle operazioni affidate;
  - copie di dati personali su supporti amovibili sono permesse solo se parte del trattamento, copie di dati sensibili devono essere espressamente autorizzate dal responsabile del trattamento. In ogni caso tali supporti devono avere un'etichetta che li identifichi e non devono mai essere lasciati incustoditi;
  - in caso si constati o si sospetti un incidente di sicurezza deve essere data immediata comunicazione al responsabile del trattamento;
- segnalare al titolare o al responsabile eventuali circostanze che rendano necessario od opportuno l'aggiornamento delle predette misure di sicurezza al fine di ridurre al minimo i rischi di distruzione o perdita,

Prot. n. **allegato 9**

anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
- effettuare la comunicazione e la diffusione dei dati esclusivamente ai soggetti indicati dal titolare o dal responsabile e secondo le modalità stabilite dai medesimi;
- mantenere, salvo quanto precisato al punto precedente, la massima riservatezza sui dati
- personali dei quali si venga a conoscenza nello svolgimento dell'incarico, per tutta la durata del medesimo ed anche successivamente al termine di esso;
- svolgere, in ogni caso, il trattamento dei dati personali per le finalità e secondo le modalità
- stabilite, anche in futuro, dal titolare e dal responsabile e, comunque, in modo lecito e secondo correttezza;
- fornire al titolare o al responsabile, a semplice richiesta e secondo le modalità indicate da questi, tutte le informazioni relative all'attività svolta, al fine di consentire loro di svolgere efficacemente la propria attività di controllo;
- in generale, prestare la più ampia e completa collaborazione al titolare ed al responsabile al fine di compiere tutto quanto sia necessario ed opportuno per il corretto espletamento dell'incarico nel rispetto della normativa vigente;
- rispettare, nella conservazione, le misure di sicurezza predisposte. In ogni operazione di trattamento dovrà essere garantita la massima riservatezza;
- verificare, in caso di allontanamento anche temporaneo dal posto di lavoro, che terzi, anche se dipendenti, non possano accedere a dati non di loro pertinenza chiudendo classificatori, cassetti e porta dell'ufficio dove i dati vengono mantenuti ed inserendo password su salvaschermo del PC;
- consegnare i documenti direttamente all'interessato utilizzando cartelline o buste non trasparenti;
- inviare telefax e posta elettronica con utilizzo della dicitura di cui in allegato 1;

L'incaricato prende atto che opererà sotto la diretta autorità del Titolare o del Responsabile, i quali avranno facoltà di revocare in ogni momento il presente incarico, senza che l'incaricato possa avanzare eventuali pretese e fatto salvo il risarcimento del danno eventualmente subito. Le revoche
saranno effettuate con effetto immediato e senza obbligo di preavviso.

5 a Attuazioni pratiche - Docenti
Linee guida in materia di sicurezza per il docente incaricato del trattamento
Vengono di seguito indicate le misure operative da adottare per garantire la sicurezza dei dati personali :
- Custodire in apposito armadio, o cassetto, dotati di serratura i seguenti documenti:
    1. Registro personale.
- Consegnare alla segreteria per l'inserimento nel fascicolo personale contenente i dati sensibili:
    1. Certificati medici esibiti dagli alunni a giustificazione delle assenze
    2. Qualunque altro documento contenente dati personali o sensibili degli alunni

Verificare la corretta funzionalità dei meccanismi di chiusura dell'armadio, segnalando tempestivamente al responsabile di sede eventuali anomalie.
- Seguire le istruzioni del docente responsabile dell'aula di informatica.
- Seguire le istruzioni del docente responsabile di sede nel caso di trattamento dei dati personali per fini diversi da quelli relativi ai punti 1 e 2.
- Tutte le comunicazioni indirizzate agli uffici, ad altro personale della scuola e al dirigente scolastico debbono essere consegnate in busta chiusa al responsabile di sede o al protocollo della sede centrale. Non è consentito, se non espressamente autorizzato, l'utilizzo del fax, della posta elettronica e dei collegamenti alla rete internet per il trattamento dei dati personali.

Per i docenti che utilizzano l'aula di informatica (nel caso di trattamento di dati personali) e per il responsabile dell'aula di informatica:
Seguire le seguenti istruzioni operative per l'utilizzo dei personal computers:
- Non lasciare floppy disk, cartelle o altri documenti a disposizione di estranei;
- Non consentire l'accesso ai dati a soggetti non autorizzati;
- Riporre i supporti in modo ordinato negli appositi contenitori e chiudere a chiave classificatori e armadi dove sono custoditi;
- Scegliere una password con le seguenti caratteristiche:
    1. originale
    2. composta da otto caratteri
    3. che contenga almeno un numero

Prot. n. **allegato 9**

4. .che non sia facilmente intuibile, evitando il nome proprio, il nome di congiunti, date di nascita e comunque riferimenti alla propria persona o lavoro facilmente ricostruibili

- curare la conservazione della propria password ed evitare di comunicarla ad altri;
- cambiare periodicamente (almeno una volta ogni tre mesi) la propria password;
- modificare prontamente (ove possibile) la password assegnata dal custode delle credenziali;
- trascrivere su un biglietto chiuso in busta sigillata e controfirmata la nuova password e consegnarla al custode delle credenziali;
- spegnere correttamente il computer al termine di ogni sessione di lavoro;
- non abbandonare la propria postazione di lavoro senza aver spento la postazione di lavoro o aver inserito uno screen saver con password;
- comunicare tempestivamente al Titolare o al Responsabile qualunque anomalia riscontrata nel funzionamento del computer;
- utilizzare le seguenti regole per la posta elettronica:
  1. non aprire documenti di cui non sia certa la provenienza
  2. non aprire direttamente gli allegati ma salvarli su disco e controllarne il contenuto con un antivirus
  3. controllare accuratamente l'indirizzo dei destinatario prima di inviare dati personali.

5 b Attuazioni pratiche - ATA

Linee guida in materia di sicurezza per il docente incaricato del trattamento

5.1 Dati personali
Il formato dei dati è fondamentalmente di due tipi: cartaceo ed informatico. Indipendentemente dal formato, il concetto di sicurezza si riferisce a tre aspetti distinti:

- **riservatezza:** prevenzione contro l'accesso non autorizzato alle informazioni:
- **integrità:** le informazioni non devono essere alterabili da incidenti o abusi;
- **disponibilità** il sistema deve essere protetto da interruzioni impreviste.

IL raggiungimento di questi obiettivi richiede non solo l'utilizzo di appropriati strumenti tecnologici, ma anche opportuni meccanismi organizzativi e procedurali; misure soltanto tecniche non sono sufficienti.
In particolare le precauzioni di tipo tecnico possono proteggere le informazioni durante il loro transito attraverso i sistemi , o anche quando queste rimangono inutilizzate su un disco di un computer; nel momento in cui esse raggiungono l'utente finale, la loro protezione dipende esclusivamente da quest'ultimo, e nessuno strumento tecnologico può sostituirsi al suo senso di responsabilità e al rispetto delle norme.

5.2 Linee giuda per la sicurezza generale

1. **Utilizzare le chiavi**
   Il primo livello di protezione di qualunque sistema è quello fisico; è vero che una porta chiusa in molti casi non costituire una protezione sufficiente, ma è anche vero che pone se non altro un primo ostacolo;
2. **Attenzione ai documenti importanti**
   E'opportuno che i documenti importanti dal punto di vista della privacy vengano archiviati negli appositi luoghi dotati di sistema di sicurezza al termine della giornata lavorativa, mentre durante l'attività devono essere custoditi con attenzione per evitare che posano essere letti da estranei anche in vostra presenza;
3. **Uso di carta riciclata**
   L'uso di carta riciclata è sicuramente una buona prassi, alla quale però è necessario prestare molta attenzione in caso si presenza di dati personali.
4. **Distruzione di documenti**
   Quando dovete disfarvi di documenti contenenti dati personali, fatelo in modo che i dati ivi contenuti risultino totalmente illeggibili.
5. **Conservazione dei documenti**
   I documenti contenenti dati personali devono essere conservati in modo tale da evitarne l'accesso a chi non ne è autorizzato. Devono altresì essere disponibili in caso di richiesta da parte dell'interessato, ma solo dietro specifica autorizzazione del Responsabile del trattamento ed entro i limiti stabiliti dalla legge;
6. **Certificazione e documenti vari**
   Limitare le produzioni di modulistica troppo vasta contenente campi quali *altro* che richiedono dati eccedenti, che esulano dalla finalità della richiesta stessa.
7. **Certificati medici vari**

Prot. n. **allegato 9**

Certificati di malattia, certificati di pronto soccorso e tutta la documentazione inerente allo stato di salute di un interessato è considerato dato sensibile *ed è trattato con una disciplina ancora più stringente rispetto al dato personale.* Se un dipendente /utente vi consegna un certificato medico, non lasciatelo sulla scrivania e portatelo al più presto all'ufficio competente.

5.2.1 procedure da attivare per i fascicoli personali – alunni e personale

Per ogni fascicolo degli alunni / personale gli incaricati al trattamento procederanno come segue:

1. Esame di tutti i documenti contenuti nel F. P.
2. catalogare i documenti esaminati, con la distinzione dei documenti contenenti dati personali da quelli contenenti dati sensibili e giudiziari;
3. i dati sensibili e giudiziari vanno collocati in un sottofasciolo chiuso in tutti e quattro i lati
4. tutti gli armadi devono essere dotati di chiavi;
5. le chiavi non devono essere lasciate incustodite;
6. al termine dell'attività di servizio tutte le chiavi vanno riposte, a cura di un incaricato, nella cassaforte della segreteria;
7. si deve limitare il trattamento dei dati sensibili e giudiziari alle sole informazioni ed operazioni individuate per le operazioni necessarie alla specifica necessità;
8. indicare anche quale è la struttura principale incaricata di tale trattamento ed eventualemente altre strutture coinvolte;
9. una volta ogni tre mesi il responsabile del trattamento dei dati procede ad una verifica a campione della corretta gestione dei fascicoli, gli incaricati devono inoltre indicare al responsabile del trattamento eventuali rischi che i dati contenuti nell'archivio possano essere diffusi. Bisogna individuare tutti i rischi possibili che corrono i dati trattati dall'istituto cercando d'inserire anche eventuali rischi specifici della scuola, magari legati allo specifico territorio, o condizione ambientale. Ovviamente per ogni evento è possibile indicare una serie di contro misure.

5.3 La sicurezza informatica

1. **Conservare i floppy, cdrom in luoghi sicuri**
   Per i dischetti e cdrom si applicano gli stessi criteri che per i documenti cartacei, con l'ulteriore pericolo che il loro smarrimento o furto può passare più facilmente inosservato, vanno riposti sotto chiave non appena avete finito d'usarli.
2. **Utilizzate le password**
   Vi sono diverse pass. Con funzioni diverse, la pass. d'accesso al computer impedisce l'utilizzo improprio della postazione; la pass. d'accesso alla rete impedisce che l'eventuale accesso non autorizzato ad una postazione renda disponibili tutte le risorse dell'ufficio; la pass. dei programmi specifici permettere di restringere l'accesso ai dati al solo personale autorizzato; la pass. Del salvaschermo impedisce che in un momento d'assenza sia possibile ad un estraneo di visualizzare il lavoro. Le passwords si scelgono in base alle indicazioni fornite dall'amministratore del sistema.
3. Attenzione alle stampe dei documenti riservati, persone non autorizzate non possono accedere alle stampe, se la stampante non si trova sulla scrivania , ci si deve recare immediatamente a ritirare le stampe: distruggere personalmente le stampe quando non servono più.
4. Non va lasciata traccia dei dati riservati.
5. I PC portatili sono facile bersaglio per i ladri, se i dati riservati devono essere gestiti su un portatile, il backup deve essere molto frequente.
6. Le passwords vanno custodite in luogo sicuro.
7. Il proprio computer non deve essere usato da personale esterno.
8. Non devono essere utilizzati apparecchi non autorizzati.
9. Non si devono installare programmi non autorizzati, solo i programmi istituzionali o acquistati dall'amministrazione con regolare licenza, sono autorizzati. Se il lavoro richiede l'utilizzo di programmi specifici, bisogna consultarsi col responsabile della sicurezza informatica.
10. Le istruzioni per la prevenzione da infezione di virus va applicata con cura.
11. Le norme fissaste per il backup vanno controllate
12. Le informazioni sensibili e non, non vanno registrate sul disco locale, ma sull'unità di rete per la quale s'effettua giornalmente il backup.

5.4 Linee guida per la prevenzione dei virus

Per gli elaboratori che ospitano archivi (o hanno accesso tramite la rete) con dati personali sono adottate le seguenti misure:

Prot. n. **allegato 9**

1. l'accesso agli incaricati ed agli addetti alla manutenzione è possibile solo in seguito ad autorizzazione scritta;
2. gli hard disk non sono condivisi in rete se non temporaneamente per operazioni di copia;
3. tutte le operazioni di manutenzione che sono effettuate on-site avvengono con la supervisione dell'incaricato del trattamento o di un suo delegato;
4. le copie di backup sono realizzate su Server e disco fisso esterno e sono conservate in Presidenza;
5. divieto per gli utilizzatori di strumenti elettronici di lasciare incustodito, o accessibile, lo strumento elettronico stesso. A tale riguardo, per evitare errori e dimenticanze, è adottato uno screensaver automatico dopo 10 minuti di non utilizzo, con ulteriore password segreta per la prosecuzione del lavoro;
6. divieto di installazione di software di qualsiasi tipo sui personal computer che contengono archivi con dati sensibili senza apposita autorizzazione scritta da parte del responsabile del trattamento dati;
7. divieto di installazione sui personal computer di accessi remoti di qualsiasi tipo mediante modem e linee telefoniche.

Si allega:

1. testo da allegare ai fax.

Da inserire nella COPERTINA DEL FAX

Le informazioni contenute nella presente comunicazione e i relativi allegati possono essere riservate e sono, comunque, destinate esclusivamente alle persone o alla Società sopraindicati.
La diffusione, distribuzione e/o copiatura del documento trasmesso da parte di qualsiasi soggetto diverso dal destinatario è proibita, sia ai sensi dell'art. 616 c.p. , che ai sensi del D. Lgs. n. 196/2003.
Se avete ricevuto questo messaggio per errore, vi preghiamo di distruggerlo e di informarci immediatamente per telefono allo _____ o inviando un messaggio all'indirizzo: _____
In caso di ricezione mancata o incompleta, telefonare al numero _____

2. allegato B, schede ex DM 305, 2006 e incarichi istituto – allegato 9 bis