D. Lgs. 196/2003

"Codice in materia di protezione dei dati personali" – *cd.* "*Privacy*".

Manuale per la Gestione in Sicurezza dei dati

Ad uso degli incaricati Ata

Titolare del Trattamento f.to Prof. ssa Patrizia DI FRANCO

Responsabile del Trattamento f.to dott. Giovanni COLUCCI

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:
   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 Patrizia DI FRANCO	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 Dott. Giovanni COLUCCI	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 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.
Incaricato del Trattamento	A.A.T, C.S.	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 l'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:

a) 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;
b) trattare i soli dati la cui conoscenza sia necessaria e sufficiente per lo svolgimento delle operazioni da effettuare;
c) 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;
d) con specifico riferimento agli atti e documenti cartacei contenenti dati personali ed alle loro copie, restituire gli stessi al termine delle operazioni affidate;
e) 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;
f) 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, 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 Attuazioni pratiche

5.1 I 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 gli opportuni meccanismi organizzativi e procedurali; misure soltanto tecniche, per quanto possano essere sofisticate, non saranno efficienti se non usate propriamente.

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 guida per la sicurezza generale

1. **UTILIZZATE LE CHIAVI**
   Il primo livello di protezione di qualunque sistema è quello fisico; è vero che una porta chiusa può 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**
   I documenti importanti dal punto di vista della privacy è opportuno che 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 possano 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 di presenza di dati personali.

4. **DISTRUZIONE DEI 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 è autorizzato. Devono altresì essere resi 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. **CERTIFICATI E DOCUMENTI VARI**
   Limitare la produzioni di modulistica troppo vasta contenete campi quali "altro" che richiedono dati eccedenti, che esulano dalla finalità della richiesta stessa.

7. **CERTIFICATI MEDICI VARI**
   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 personale 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 sottofascicolo chiuso in tutti e quattro i lati;
4. tutti i classificatori devono essere dotati di apposite chiavi;
5. le chiavi vanno custodite dagli incaricati;
6. al termine dell'attività di servizio tutte le chiavi vanno risposte a cura di un incaricato nella cassaforte della segreteria ovvero vanno consegnate ai collaboratori scolastici per la relativa

custodia;

7. poiché nei documenti è necessario indicare la natura dei dati trattati (Sensibili e/o Giudiziari) e la natura dei dati trattati è relativa solo al trattamento e non a tutte le tipologie di dati presenti all'interno della banca dati; è possibile che alcuni dati sensibili non sia necessario tenerli quindi nella classificazione dei documenti è possibile riconsegnare gli stessi al personale interessato.
8. indicare anche qual è la struttura principale incaricata di tale trattamento ed infine, se presenti, altre strutture sempre incaricate del medesimo trattamento (ad esempio dati trattati dall'ufficio didattica e dal personale docente.
9. Tutti i fascicoli personale dell'archivio corrente entro il 31 dicembre di ogni anno devono pertanto essere riesaminati dagli incaricati al trattamento;
10. Il responsabile del trattamento dei dati procede ad una verifica a campione al 31marzo di ogni anno e periodicamente almeno una volta ogni 3 mesi.

Gli incaricati devono inoltre indicare al responsabile del trattamento eventuali rischi che i dati
contenuti nell'archivio possano essere diffusi. Bisogna individuare tutti i possibili rischi che corrono i dati trattati dall'istituto cercando di 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 contromisure con le quali s'intende arginarlo.

5.3 La sicurezza informatica

1. CONSERVATE IN UN LUOGO SICURO

Per i supporti di archiviazione si applicano gli stessi criteri che per i documenti cartacei, con l'ulteriore pericolo che il loro smarrimento (che può anche essere dovuto a un furto) può passare più facilmente inosservato. A meno che non siate sicuri che contengano solo informazioni non sensibili, riponeteli sotto chiave non appena avete finito di usarli.

2. UTILIZZATE LE PASSWORD

Vi sono svariate categorie di password, ognuna con il proprio ruolo preciso:

La password di accesso al computer impedisce l'utilizzo improprio della vostra postazione, quando per un motivo o per l'altro non vi trovate in ufficio.

La password di accesso alla rete impedisce che l'eventuale accesso non autorizzato a una postazione renda disponibili tutte le risorse dell'Ufficio.

La password dei programmi specifici permette di restringere l'accesso ai dati al solo personale autorizzato.

La password del salvaschermo, infine, impedisce che una vostra assenza momentanea permetta a una persona non autorizzata di visualizzare il vostro lavoro.

Scegliete le password secondo le indicazioni fornite dall'Amministratore del Sistema.

3. ATTENZIONE ALLE STAMPE DI DOCUMENTI RISERVATI

Non lasciate accedere alle stampe persone non autorizzate; se la stampante non si trova
sulla vostra scrivania recatevi quanto prima a ritirare le stampe. Distruggete personalmente le stampe quando non servono più.

4. NON LASCIATE TRACCIA DEI DATI RISERVATI

5. PRESTATE ATTENZIONE ALL'UTILIZZO DEI PC PORTATILI

I PC portatili sono un facile bersaglio per i ladri. Se avete necessità di gestire dati riservati su un portatile, fatevi installare un buon programma di cifratura del disco rigido, e utilizzate una procedura di backup periodico.

6. CUSTODITE LE PASSWORD IN UN LUOGO SICURO

7. NON FATE USARE IL VOSTRO COMPUTER A PERSONALE ESTERNO A MENO DI NON ESSERE SICURI DELLA LORO IDENTITÁ

8. NON UTILIZZATE APPARECCHI NON AUTORIZZATI

L'utilizzo di modem senza una specifica autorizzazione su postazioni di lavoro collegati alla rete offre una porta d'accesso dall'esterno non solo al vostro computer, ma a tutta la Rete, ed è quindi vietata. Per l'utilizzo di altri apparecchi, consultatevi con il responsabile IT.

9. NON INSTALLATE PROGRAMMI NON AUTORIZZATI

Solo i programmi istituzionali o acquistati dall'Amministrazione con regolare licenza sono autorizzati. Se il vostro lavoro richiede l'utilizzo di programmi specifici, consultatevi con il responsabile IT.

10. APPLICATE CON CURA LE LINEE GUIDA PER LA PREVENZIONE DA INFEZIONI DI VIRUS

La prevenzione da virus sul vostro computer è molto più facile e comporta uno spreco di tempo molto minore della correzione degli effetti di un virus; tra l'altro, potreste incorrere in una perdita irreparabile di dati.

11. CONTROLLATE LA POLITICA LOCALE RELATIVA AI BACKUP

Evitate di registrare nel disco locale informazioni sensibili e non in quanto esse non vengono salvate, e a fronte di un guasto tecnico irrimediabilmente perse. La registrazione sulle unità di rete invece avviene in sicurezza in quanto i dati vengono salvati giornalmente.

5.4 Linee guida per la prevenzione dei virus

1. USATE SOLTANTO PROGRAMMI PROVENIENTI DA FONTI FIDATE

Copie sospette di programmi possono contenere virus o altro software dannoso. Ogni programma deve essere sottoposto alla scansione prima di essere installato. Non utilizzate programmi non autorizzati, con particolare riferimento ai videogiochi, che sono spesso utilizzati per veicolare virus.

2. PROTEGGETE I VOSTRI DISCHETTI DA SCRITTURA QUANDO POSSIBILE

In questo modo eviterete le scritture accidentali, magari tentate da un virus che tenta di propagarsi. I virus non possono in ogni caso aggirare la protezione meccanica.

5. ASSICURATEVI CHE IL VOSTRO SOFTWARE ANTIVIRUS SIA AGGIORNATO

6.NON DIFFONDETE MESSAGGI DI PROVENIENZA DUBBIA