

Regolamento scolastico interno sul corretto trattamento dei dati personali e sulle misure di sicurezza

Premesso

1) Che ai sensi del Decreto Legislativo n. 196 del 2003, i dati possono essere classificati come segue:

- **Personali**: ovvero qualsiasi informazione che riguardi persone, società, enti, associazioni identificati o che possano essere identificati anche attraverso altre informazioni quali, ad esempio, un numero o un codice identificativo. Sono dati personali: nome e cognome o denominazione; indirizzo o sede; codice fiscale o partita iva, foto, registrazione della voce di una persona, la sua impronta digitale o vocale, o qualsiasi altra ripresa audiovisiva. La persona difatti può essere identificata anche attraverso altre notizie che non siano direttamente identificative (ad esempio, associando la registrazione della voce di una persona alla sua immagine, oppure alle circostanze in cui la registrazione è stata effettuata: luogo, ora, situazione).

- **Sensibili**: dati personali che, per la propria delicatezza, richiedono particolari cautele; essi sono quei dati idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

- **Giudiziari**: dati personali idonei a rilevare provvedimenti emessi dalle Autorità Giudiziarie e contenuti nel casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reati e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli artt. 60 e 61 c.p.p..

2) Che le informazioni possono essere classificate come segue:

- **Pubblica**: informazione generale esplicitamente rivolta anche a comunicazione o diffusione indifferenziata all'esterno dell'Istituto scolastico.

- **Comune**: informazione generale da ritenersi riservata al solo Istituto scolastico; può essere conosciuta anche da soggetti esterni purché indicati esplicitamente tra i destinatari.

- **Riservata**: informazione rivolta a specifici soggetti destinatari.

3) Che ai sensi del Decreto Legislativo n. 196 del 2003, l'Istituto scolastico, come gli altri soggetti pubblici, salvo quelli economici,

- tratta **dati personali** qualora sia necessario per lo svolgimento delle funzioni istituzionali, anche qualora non sussista il consenso del soggetto interessato, ed in assenza di una espressa norma di legge o di regolamento;

- tratta **dati sensibili** qualora sussista una esplicita previsione normativa che espliciti la legittimazione al trattamento e indichi i dati trattabili, le operazioni realizzabili e lo scopo seguito, connotato da un rilevante interesse pubblico. Qualora invece non siano indicati i tipi di dati sensibili e operazioni eseguibili, ma sia specificato dalle disposizioni legislative soltanto lo scopo di rilevante interesse pubblico, gli elementi

mancanti dovranno essere identificati e resi pubblici dalle singole Amministrazioni con regolamenti adottati in conformità al parere espresso dal Garante. Se al contrario non sussiste una norma legislativa, l'Ente dovrà richiedere al Garante di dichiarare la sussistenza di un interesse pubblico rilevante connesso agli scopi del trattamento a cui vuol procedere e successivamente dovrà identificare e rendere pubblici i tipi di dati e di operazioni.

- tratta **dati giudiziari** soltanto se autorizzato da espressa norma di legge o provvedimento del Garante che determinino, oltre allo scopo di rilevante interesse pubblico, la tipologia dei dati trattati ed il tipo di operazioni eseguibili. Qualora invece non siano indicati i tipi di dati giudiziari e i tipi di operazioni eseguibili, ma sia specificato dalle disposizioni legislative soltanto lo scopo di rilevante interesse pubblico, gli elementi mancanti dovranno essere identificati e resi pubblici dalle singole Amministrazioni con regolamenti statuari adottati in conformità al parere espresso dal Garante.

- tratta **dati giudiziari e sensibili** indispensabili per svolgere attività istituzionali che non possono essere adempiute attraverso il trattamento di dati anonimi o personali di diversa natura. La Scuola dovrà verificarne periodicamente l'esattezza, la completezza ed eventualmente procedere al loro aggiornamento. Dovrà inoltre verificare che i dati siano pertinenti, necessari e non eccedenti rispetto agli scopi stabiliti; qualora non lo siano, i dati non potranno essere utilizzati. La Scuola non potrà utilizzare tali dati per test psicoattitudinali e potrà confrontare i dati relativi ad un soggetto soltanto se i motivi dell'operazione risultino da un atto scritto. Potrà procedere invece alla diffusione dei dati e le operazioni di raffronto ottenuto con l'incrocio di banche dati di vari soggetti solo se previsto da disposizioni di legge.

- tratta, con particolare cautela ed attenzione, i dati atti a rilevare lo stato di salute e vita sessuale, eventualmente attraverso cifratura o codici identificativi, se tali dati sono trattati elettronicamente in apposite banche dati. In ogni caso, tali dati saranno archiviati in modo separato dagli altri e, in special modo, quelli sulla salute non possono essere diffusi.

4) Che ai sensi del Decreto Legislativo n. 196 del 2003, per **trattamento dei dati** si intende "qualunque operazione o complesso di operazioni concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione dei dati". In tale ottica è indifferente che le operazioni vengano svolte con o senza l'ausilio di mezzi elettronici, o comunque automatizzati, per cui anche i trattamenti effettuati su supporto cartaceo sono assoggettati alla normativa privacy. Pertanto le operazioni di trattamento si possono idealmente suddividere in tre macro-tipologie, in funzione del fatto che il loro fine sia:

1. Il reperimento delle informazioni.

Tale fase è tecnicamente definita raccolta di dati, ovvero l'acquisizione delle informazioni, in qualunque modo essa avvenga: ad esempio, direttamente dalla persona interessata, presso terzi, o mediante consultazione di elenchi.

2. Il trattamento "interno" delle informazioni.

Si raggruppano in tale macro-tipologia le varie operazioni, poste in essere da chi raccoglie informazioni per organizzarle e renderle agevolmente usufruibili. Esse sono:

- la registrazione dei dati, cioè il loro inserimento in supporti, automatizzati o manuali, al fine di rendere i dati disponibili per i successivi trattamenti,
- la organizzazione dei dati in senso stretto, cioè il processo di lavorazione che ne favorisca la fruibilità attraverso l'aggregazione o la disaggregazione, l'accorpamento, la catalogazione eccetera,
- la elaborazione, ovvero le operazioni che attribuiscono significatività ai dati in relazione allo scopo per il quale essi sono stati raccolti,
- la selezione, la estrazione ed il raffronto, specifiche che rientrano nella ipotesi più generale della elaborazione,
- la modificazione dei dati registrati, in relazione a variazioni o a nuove acquisizioni,
- la interconnessione, ovvero la messa in relazione di banche dati diverse e distinte tra loro al fine di compiere ulteriori processi di elaborazione, selezione, estrazione o raffronto,
- il blocco, ovvero la conservazione dei dati con sospensione temporanea dei trattamenti,
- la conservazione dei dati, alla quale la legge dedica particolari attenzioni sotto il profilo della sicurezza,
- la cancellazione o la distruzione dei dati, anch'esse operazioni il cui compimento fa sorgere l'obbligo di effettuare taluni adempimenti.

3. L'uso delle informazioni nei rapporti con l'esterno.

Tale tipologia di intervento, poiché comporta una comunicazione di dati personali verso terzi, è particolarmente delicata, in quanto è con essa che si può concretamente ledere la sfera della privacy altrui.

L'utilizzo di tali strumenti può essere diverso:

- diretto, instaurando cioè un rapporto con la persona sul conto della quale si sono raccolte informazioni,
- ovvero consistere nel mettere a disposizione di terzi le informazioni raccolte.

Le operazioni di utilizzo cui la legge dedica le maggiori attenzioni, in quanto si tratta di quelle potenzialmente più lesive della privacy, sono quelle con cui si mettono a disposizione di terzi i dati personali.

Esse sono:

- la comunicazione, cioè il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, in qualunque forma, anche mediante la loro messa a disposizione o consultazione,
- la diffusione, cioè il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

5) Che ai sensi del Decreto Legislativo n. 196 del 2003, la Scuola dovrà fornire ai soggetti, i cui dati vengono trattati, un informativa ai sensi dell'art 13 del Decreto.

6) che per lo svolgimento delle quotidiane attività lavorative, la Scuola necessita in numerosi ruoli e posizioni organizzative dell'utilizzo di apparecchiature informatiche. L'uso di tali apparecchiature deve essere disciplinato da norme certe in quanto da comportamenti - anche inconsapevolmente non leciti -

possono derivare conseguenze gravi, sia sul piano tecnico (come un blocco della funzionalità o una perdita di dati) che sul piano giuridico (mediante l'insorgere di responsabilità sia penali che civili a carico contestualmente del Dirigente Scolastico e del personale docente ed amministrativo).

Ciò premesso, allo scopo di chiarire definitivamente le norme di comportamento, viene emanato il seguente **Regolamento Interno**, affinché i dipendenti della segreteria e i docenti evitino di porre in essere inconsapevoli comportamenti incompatibili con la correttezza professionale richiesta e/o con il corretto svolgimento della prestazione professionale da parte degli stessi. **Occorre, pertanto, che ciascuno si uniformi al rispetto delle seguenti regole al fine di adempiere correttamente alle disposizioni legislative.**

Quanto segue è redatto nel pieno rispetto delle leggi regolatrici i rapporti di lavoro ed è peraltro affisso a far data dal 15/09/2009 nelle bacheche utilizzate per le informazioni ai dipendenti.

Utilizzo strumentazione

- 1) La strumentazione intesa come insieme di Hardware e Software messa a disposizione dei dipendenti deve essere utilizzata e conservata appropriatamente; della stessa deve essere fatto un uso conforme ed esclusivamente circoscritto alle attività professionali cui ciascuno è preposto.
- 2) La strumentazione non deve essere utilizzata per scopi personali.
- 3) E' fatto divieto di installare sulla strumentazione in uso, hardware fisso o removibile qualora ciò non risulti espressamente richiesto ed autorizzato dal responsabile della Privacy. Pertanto, l'Ente scolastico si riserva di eliminare qualsiasi elemento hardware la cui installazione non sia stata appositamente prevista o autorizzata.
- 4) In caso di allontanamento dalla propria postazione hardware, è fatto obbligo all'utente di attivare il salvaschermo protetto da password o il lock per il terminale.

Accesso ed uso dei sistemi

- 1) Le unità disco (locali o di rete) sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia connesso all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità.
- 2) Il personale amministrativo o docente si connette alla rete tramite autenticazione univoca personale, che gestisce in autonomia ed ha responsabilità delle proprie password. In nessun caso devono essere annotate password in chiaro sia su supporto cartaceo che informatico. I requisiti minimi di complessità delle password sono:
 - redazione con caratteri maiuscoli e/o minuscoli;
 - possono essere inclusi simboli, numeri, punteggiatura e lettere;

- numericamente devono essere password di almeno 8 caratteri (ad eccezione dei sistemi operativi che non supportano tali requisiti);

- non deve trattarsi di password basate su informazioni personali, riferimenti familiari o comunque dati inerenti direttamente il soggetto titolare della password stessa.

3) Il personale amministrativo o docente ha l'obbligo di cambiare la password ogni 3 mesi come prescritto dal nuovo Codice della Privacy in relazione alle misure di sicurezza minime per il trattamento dei dati sensibili o giudiziari.

4) Il titolare della password è tenuto a non rivelare ad alcuno, colleghi e superiori inclusi, la password, dovendone avere la massima diligenza e preservandone la segretezza anche durante il momento della digitazione. Qualora il dipendente prenda coscienza che taluno può aver visionato la digitazione o essere comunque a conoscenza della password, deve immediatamente cambiarla. Qualora sia richiesto di riferire in qualunque forma la password, ovvero telefonicamente, via e-mail, localmente il dipendente è obbligato a rifiutarsi; contemporaneamente deve dare immediata comunicazione dell'accaduto al Responsabile per il trattamento dati personali.

5) Non debbono essere utilizzate nella configurazione delle caselle di posta elettronica le opzioni di "compilazione automatica" o remember password, presenti nei browser o in altre applicazioni.

6) Ogni incaricato sarà custode e responsabile delle proprie password. In ogni caso egli avrà cura di consegnare ogni 3 mesi, in busta chiusa al custode delle password, le proprie credenziali di autenticazione per l'accesso al proprio sistema informatico (ID e PW). Il custode sarà autorizzato ad aprire le buste consegnate solo in caso di urgente necessità, determinata dall'assenza prolungata dal lavoro dell'incaricato. In caso di apertura e di utilizzo delle ID e PW altrui, il custode avrà cura di avvertire l'incaricato assente, che dovrà modificare le ID e PW al suo rientro al lavoro.

Installazione programmi

1) Sul pc in uso non devono essere installati programmi che non siano ufficialmente forniti dal Titolare, dal Responsabile o dal Manutentore, dei quali non sia, espressamente e per iscritto, autorizzata l'installazione mediante la stesura di una nuova versione del documento di mappatura del software.

2) E' vietato scaricare per scopi personali o scolastici programmi reperiti in rete o da qualunque altra sorgente esterna, salvo espressa autorizzazione del Titolare, Responsabile o Manutentore.

3) L'Istituto scolastico, peraltro, ricorda all'utilizzatore che costituiscono illecito penale le condotte consistenti nella illecita duplicazione o riproduzione di software ai sensi della legge sul diritto d'autore n. 633/41 come novellata, art. 171 bis.

Utilizzo supporti magnetici e dati

1) È fatto obbligo di conservare, custodire e controllare i registri cartacei ed i supporti informatici removibili contenenti dati, informazioni, notizie o immagini di attinenza al proprio lavoro, affinché nessun soggetto terzo ne prenda visione o possesso.

2) E' fatto divieto di utilizzare supporti magnetici o ottici non espressamente forniti dalla scuola.

3) Qualsiasi file estraneo all'attività lavorativa o non espressamente autorizzato, non può, nemmeno in via transitoria, essere salvato sul pc in uso del dipendente.

Utilizzo rete interna

1) La rete interna, istituita appositamente per permettere collegamenti funzionali tra dipendenti che prestano servizio all'interno della scuola, non può essere utilizzata per scopi diversi da quelli ai quali è destinata, senza espressa autorizzazione del Dirigente Scolastico.

2) E' fatto divieto di far circolare internamente alla rete della scuola file non espressamente autorizzati né alcuna altra notizia, informazione o dato non inerente l'attività scolastica.

3) Qualora nella rete interna debbano circolare dati, notizie ed informazioni, inerenti la scuola, deve essere premura di ciascun dipendente preservare gli stessi dalla conoscibilità di terzi soggetti non espressamente autorizzati ad aver notizia di tali dati.

Utilizzo rete esterna Internet

1) E' fatto divieto ai dipendenti di navigare in siti non attinenti all'attività scolastica, in quanto l'utilizzo al collegamento ad Internet deve essere funzionale all'attività lavorativa.

2) Sono interdette partecipazioni a mailing list, forum, chat o altri mezzi di comunicazione telematica non attinenti all'attività lavorativa, attuate mediante pc, salvo espressa autorizzazione del Dirigente Scolastico.

3) E' vietato utilizzare la rete ai fini di operazioni di "remote banking" personali non attinenti con l'attività della scuola. È parimenti vietato effettuare transazioni on line di qualsiasi genere salvo espressa autorizzazione.

4) E' fatto divieto di memorizzare dalla rete documenti, file o dati comunque non attinenti allo svolgimento delle attività scolastiche.

5) Si rende noto che il Dirigente Scolastico può, in qualunque momento e senza preavviso, attivare meccanismi di monitoraggio delle attività di rete per fini organizzativi e funzionali o di controllo della sicurezza dell'impianto. Gli archivi di log risultanti da questo monitoraggio contengono traccia di ogni operazione di collegamento effettuata dall'interno della scuola verso Internet.

L'utilizzo dei software di protezione

Il sistema adottato dalla scuola presenta software di protezione che vengono aggiornati automaticamente. Si raccomanda al personale amministrativo e docente di verificare periodicamente l'effettivo funzionamento del sistema (verifica dei files e aggiornamenti dell'antivirus) e di avvisare l'incaricato alla manutenzione del sistema informatico qualora il software evidenzia un virus. In questo caso il files deve essere isolato (messo in quarantena) in attesa di verifica dell'incaricato del sistema informatico e della successiva eliminazione definitiva dal sistema.

Si sottolinea, comunque, l'importanza di controllare preventivamente tutti i files provenienti dall'esterno e di adottare diligentemente le opportune cautele al momento della trasmissione all'esterno di nostri files.

Utilizzo del fax

1) Il fax deve essere utilizzato per scopi puramente scolastici.

2) È fatto divieto lasciare documenti incustoditi presso le postazioni di fax.

Utilizzo posta elettronica

1) Le caselle di posta elettronica date in uso al dipendente o docente sono destinate ad un utilizzo tassativamente inerente all'attività lavorativa scolastica.

2) Si rende noto che, per motivi organizzativi e funzionali, la Scuola può archiviare i messaggi di posta elettronica, in uscita ed in entrata, e può stabilire meccanismi automatici di trasmissione in copia degli stessi ad altre caselle di posta elettronica, trattandosi di posta che la Scuola presuppone essere di natura esclusivamente lavorativa. Conseguentemente, al fine di non ledere il diritto alla riservatezza e segretezza della posta utilizzata per scopi personali, i dipendenti non dovranno utilizzare la caselle di posta elettronica per fini che esulano dal contesto lavorativo scolastico.

3) Inoltre, la Direzione comunica che in caso di assenza per qualsiasi motivo dell'utilizzatore (malattia, ferie, allontanamento temporaneo dal posto di lavoro) qualora si renda necessario, il Responsabile custode delle password (o eventualmente un delegato del Responsabile) potrà accedere alla posta elettronica del sottoscrittore al fine di non interrompere né rallentare l'attività amministrativa o didattica o semplicemente al fine di prendere visione dello storico delle comunicazioni di interesse della scuola.

4) E' fatto divieto di divulgare le notizie, i dati e qualsiasi altra informazione appresa in occasione della ricezione o invio di posta elettronica, in quanto coperte dal segreto professionale cui sono tenuti i dipendenti ed i docenti in ottemperanza agli obblighi di fedeltà e correttezza.

Custodia, conservazione e controllo documenti cartacei

1) E' fatto obbligo al dipendente o al docente di custodire il materiale cartaceo affinché nessuno ne prenda visione, possa manipolarlo o riprodurlo.

2) È fatto divieto di lasciare qualsiasi documento incustodito presso la propria postazione qualora sia previsto un allontanamento per un lasso di tempo tale da consentirne eventualmente la visione da parte di terzi.

3) È fatto divieto di lasciare incustodito qualsiasi documento in locali estranei alla propria postazione, prestando particolare attenzione a non lasciarli presso la fotocopiatrice.

Gestione, conservazione e controllo dei dati informatici

1) È fatto divieto applicare sistemi di crittografia, steganografia e simili ai dati se non espressamente autorizzati per iscritto dal Responsabile privacy.

2) È obbligo dell'utente salvare nelle apposite cartelle tutti i documenti scolastici e informare il Responsabile privacy di ulteriori necessità di riservatezza o protezione.

3) Le cartelle residenti su server saranno oggetto di verifica periodica da parte del personale addetto alla manutenzione e gestione dei Files Server che provvederà senza preavviso alla rimozione di tutti quei files ritenuti non conformi al regolamento in vigore.

4) Le eventuali cartelle condivise sui client di rete devono essere normalmente vuote e sono da considerarsi come deposito solo temporaneo dei documenti. Con cadenza almeno mensile, l'amministratore provvederà a cancellarne il contenuto senza preavviso.

5) È fatto obbligo al dipendente o docente di inserire la funzione di screen server riattivabile con inserimento password, qualora trascorrono più di 10 minuti di inattività presso la propria postazione.

Obbligo di back-up

1) Il personale amministrativo e i docenti, che usufruiscono del computer, devono effettuare un costante back-up dei dati elaborati al fine di ridurre al minimo il rischio di perdita dati in caso di black-out.

2) È fatto peraltro obbligo di effettuare il salvataggio delle informazioni nelle cartelle del proprio settore di appartenenza presso il file server, incluse quelle trattate in locale, secondo le modalità individuate costantemente dal Responsabile privacy.

Segreto professionale

1) Il personale della scuola non può divulgare, pubblicare o comunicare in alcun modo a terzi, direttamente o indirettamente, in toto o in parte, le informazioni apprese in occasione dello svolgimento delle mansioni per le quali è stato assunto, né potrà usarle, sfruttarle o disporne in proprio o tramite terzi. Nella valutazione delle informazioni, il sottoscrittore si impegna a prendere ogni misura perché le stesse rimangano segrete, essendo inteso che, in caso di divulgazione non autorizzata, sarà a carico del sottoscrittore l'onere di provare di avere adottato tali misure.

2) Il personale della scuola si impegna, altresì, a rispettare con esattezza i suddetti obblighi poiché si presume che la violazione degli impegni di segretezza contenuti nel presente accordo siano idonei a causare ingenti danni alla Scuola.

3) Gli obblighi del personale previsti in questo capo non termineranno all'atto di cessazione del rapporto di lavoro, se non in riferimento a quelle specifiche parti delle informazioni che il personale possa dimostrare che erano già di pubblico dominio al momento della conclusione del rapporto, o che lo sono diventate in seguito per fatto a lui non imputabile.

Riservatezza dati

1) Premesso che per «Informazioni Riservate» si intendono tutte le informazioni di qualsivoglia natura riferite o apprese in occasione dello svolgimento di mansioni per le quali il soggetto è stato assunto dalla Scuola, il personale amministrativo e docente si impegna a considerare le Informazioni Riservate come strettamente private e ad adottare tutte le misure necessarie per non pregiudicare la riservatezza di tali informazioni.

2) Si impegna altresì ad utilizzare le Informazioni Riservate unicamente allo scopo di effettuare lo svolgimento dell'attività cui è preposto e di conseguenza a non usare tali informazioni in alcun modo che arrechi danno alla Scuola né per alcun altro scopo di qualsiasi natura.

3) Si impegna a cancellare o distruggere qualsiasi informazione registrata sul proprio computer o altro strumento posseduto, custodito o controllato qualora cessi il rapporto esistente con la Scuola.

4) Gli impegni di cui al presente capo non proibiscono di comunicare Informazioni Riservate:

a) ad amministratori e dipendenti, avvocati, revisori, banche o altri nostri consulenti ai quali la conoscenza di tali Informazioni è necessaria al fine dell'espletamento di attività funzionali alla Scuola;

b) a soggetti diversi da quelli specificati alla precedente lettera a), qualora ciò sia stato autorizzato dal Dirigente Scolastico o dal Responsabile privacy;

c) se, al momento in cui vengono rese note, siano di pubblico dominio o se lo diventino dopo essere state rese note per causa non imputabile al dipendente;

5) L'impegno di riservatezza di cui al presente capo si protrarrà anche dopo la cessazione del rapporto di lavoro e sino a quando le informazioni in oggetto non saranno rese di pubblico dominio.

Dati personali che possono essere trattati da Docenti, personale amministrativo, collaboratori scolastici e del D.S.

Qualunque documento scolastico che contenga dati personali comuni o sensibili, per qualsiasi attività didattica ed organizzativa, deve essere sottoposto ad una qualche forma di protezione.

Dovrà essere utilizzata una particolare attenzione per tutti i dati trattati in occasione delle attività di seguito elencate:

- attività didattiche e di sorveglianza in relazione alla scelta di avvalersi dell'insegnamento della Religione Cattolica;
- registrazione di assenze per motivi di salute o familiari con visione di certificati medici di avvenuta guarigione; giustificazioni di assenza dovute a festività religiose di religioni non cattoliche;
- presa visione di certificazioni mediche per esonero da educazione con diagnosi;
- visione scrittura sul libretto personale, per le comunicazioni scuola-famiglia;
- gestione di alunni portatori di handicap e relative documentazioni per l'integrazione;
- scrittura di note disciplinari e la gestione registri contenenti tali note, i provvedimenti di sospensione ect...(in quanto l'eventuale diffusione potrebbe ledere la dignità dell'interessato ed il suo diritto alla riservatezza);
- elaborazioni di valutazioni intermedie e finali (profitto, grado di impegno, comportamento, profilo psicologico ed attitudinale) e scrittura delle stesse su moduli e registri (tali valutazioni dovranno essere riferite agli sforzi dell'allievo, non in considerazione di situazioni di salute, familiari ect..)
- gestione degli elaborati scritti (in particolare temi di italiano, riportanti in alcuni casi informazioni delicate sulla sfera personale e familiare dell'alunno);
- conoscenza ed eventuale utilizzo di informazioni su problemi di salute dell'alunno, messe a disposizione dai genitori o dall'alunno stesso, che possono presentarsi durante le lezioni, in alcuni casi con grave rischio per la sua vita (come allergie con pericolo di shock anafilattico, asma grave con pericolo di soffocamento, diabete grave, epilessia, cardiopatie gravi, ect..) o casi imbarazzanti (come disturbi di incontinenza);
- gestione dei registri di classe, del registro del docente e dei verbali del Consiglio di Classe;
- gestione dei registri e dei documenti d'esame;
- gestione dei dati comuni degli alunni in caso di visite o viaggi di istruzione;
- gestione del P.O.F. e dell'orientamento scolastico in ingresso ed in uscita (quando sono coinvolti profili psicologici).

Procedure da seguire nel trattamento dei dati

1) I registri personali devono essere custoditi dall'interessato in luogo chiuso o affidati ad incaricati di riceverli. I registri di classe devono essere consultabili solo dagli alunni della classe interessata e si devono impedire accessi non autorizzati; i collaboratori scolastici sono incaricati di riporli in luogo sicuro, alla fine delle lezioni. Qualsiasi registro, elaborato, elenco, libretto o fascicolo personale o certificato che contenga dati personali di qualcuno, va custodito con cautela, impedendo che altri ne prendano visione, lo copino o se ne impadroniscano. Il registro dei verbali dei Consigli di classe e qualunque altro registro di verbali, affidato per la scrittura, la firma o la consultazione, deve essere mantenuto protetto da accessi non autorizzati e riconsegnato quanto prima al Dirigente Scolastico o alla Segreteria.

2) I documenti ricevuti aperti vanno immediatamente consegnati in Segreteria, senza prenderne visione. Se c'è il sospetto che si tratti di certificati medici, certificazioni relative ai redditi ect., si deve dare all'interessato una busta chiusa per inserirvi il relativo documento. Prestare sempre cautela per il trasporto di documenti alla posta o ad altri destinatari e per la ricezione di documenti in entrata o da far circolare nella scuola.

3) I dati sensibili vanno protetti dalla visione di terzi, che non sia strettamente necessaria. Eventuali certificati medici vanno visionati solo se necessario e poi restituiti in Segreteria. In questi casi, se l'informazione è orale, si è tenuti al massimo riserbo; se è scritta, chiedere sempre al D.S. o al DGSA per le procedure da adottare ed agire con la massime cautela. Anche informazioni su particolari diete seguite dall'alunno o per motivi di salute o per motivi religiosi sono considerati dati sensibili, e pertanto rilevabili solo in casi strettamente necessari ed omettendone la ragione.

4) Nei casi di alunni portatori di handicap (dati di massima sensibilità, in quanto idonei a rivelare lo stato di salute) i relativi documenti dovranno essere visti dai docenti e personale strettamente necessari, conservati con elevata cautela e poi consegnati in segreteria, mettendoli in busta chiusa, su cui sarà annotato il nome dell'interessato, la descrizione del contenuto, la data e l'annotazione "da conservare separatamente in armadio sicuro"; al loro posto, insieme ad altri elaborati, si metterà un foglio con l'annotazione del luogo di conservazione.

5) I temi o elaborati vari sono raccolti direttamente dall'interessato in archivio sicuro; nei casi in cui contengano dati sensibili, vanno consegnati in busta chiusa alla segreteria e conservati a parte (annotare e gestire secondo le procedure di cui al punto 4).

6) Prestare cautela nel trattamento dei dati per le attività di recupero o integrative e per gli elenchi contenenti solo dati anagrafici; per comunicarli a terzi, soprattutto per i privati, e solo per fini istituzionali, occorre l'autorizzazione del Dirigente Scolastico.

7) E' vietato apporre foto di allievi, del singolo o di gruppi, sui registri o altro, tranne per i cartellini di identità per la partecipazione a gare sportive (previo consenso del genitore).

8) Tutti i documenti devono essere custoditi in stanze contenenti archivi, da mantenersi chiusi, ed impedire ai non incaricati di entrare. La Presidenza, Segreteria e gli uffici in genere vanno chiusi a chiave, quando non presenziati dal relativo personale.

E' fatto divieto assoluto a chiunque non ne abbia avuto esplicita autorizzazione di utilizzare i computer della Segreteria o della Presidenza o che comunque contengano dati personali. Si deve intervenire immediatamente per impedire l'accesso ai terminali a chi non è autorizzato.

Gli esterni, per motivi di manutenzione o pulizia locali, devono entrare nella stanze citate o negli archivi per i quali è prevista la chiusura a chiave, seguiti a vista.

Applicazione ed interpretazione del presente regolamento

Per qualsiasi dubbio relativo all'applicazione pratica o all'interpretazione del presente regolamento, l'utente può rivolgersi al Responsabile della privacy, nella persona che in qualsiasi tempo rivestirà tale carica o, in alternativa, al Dirigente Scolastico.

Disciplina deroghe e modifiche del presente regolamento

1) Qualora al presente regolamento risulti necessario apportare modifiche, queste saranno applicate dandone conoscenza immediata a tutto il personale docente ed amministrativo.

2) Qualora si renda necessario per qualsiasi motivo, derogare ad uno o più punti del presente regolamento, sarà obbligatorio porre per iscritto e veder accettata dal personale e dalla Scuola tale deroga, mediante specifica sottoscrizione.

Deroghe o modifiche di uno o più punti del presente regolamento, non rendono invalidi gli altri punti, salvo ipotesi di evidente incompatibilità, per cui prevarrà l'applicazione della clausola temporalmente più recente.

La violazione del suddetto regolamento può comportare responsabilità disciplinari, nonché civili e penali.

Per qualsiasi dubbio interpretativo e comportamentale circa il presente regolamento può essere chiesto l'intervento del Responsabile Privacy o del Dirigente Scolastico, nella persona in carica pro tempore.

Approvato in data 15/09/2009

Il Dirigente Scolastico

Prof. Vincenzo Nicolì