Istituto Comprensivo Statale ad Indirizzo Musicale
" Guastella - Landolina"
via Ettore Majorana snc- C.da Gabatutti – 90036 Misilmeri (Pa)
Tel. 0917525597-091546899-C.F. 97382260822
Email (PEO):PAIC8BW002@istruzione.it (PEC) PAIC8BW002@pec.istruzione.it
Sito web: https://www.icsguastellalandolina.edu.it
_____Sede dell'Osservatorio di Area sulla Dispersione Scolastica Distretto 9_____

MANUALE OPERATIVO DOCENTI

Tutela dei dati personali e gestione delle informazioni scolastiche

Indice dei capitoli

Capitolo 1 – Finalità del Manuale e contesto normativo

La gestione dei dati personali in ambito scolastico rappresenta oggi una delle aree più delicate e complesse dell'attività dei docenti. Le scuole, infatti, trattano quotidianamente una vasta quantità di informazioni relative agli studenti, alle loro famiglie e al personale scolastico: dati anagrafici, documentazione sanitaria, informazioni legate al percorso didattico, valutazioni, certificazioni, comunicazioni interne ed esterne. Tali dati, proprio perché riguardano soggetti spesso minorenni, necessitano di un livello di protezione particolarmente elevato. Da qui nasce l'esigenza di un **Manuale Operativo per i Docenti**, che fornisca indicazioni chiare e uniformi sul corretto trattamento dei dati personali, in linea con il **Regolamento Europeo 2016/679 (GDPR)** e con la normativa nazionale (D.Lgs. 196/2003 e successive modifiche).

L'obiettivo principale del manuale è duplice: da un lato, tutelare i diritti fondamentali delle persone coinvolte, garantendo che le loro informazioni siano gestite in modo lecito, sicuro e trasparente; dall'altro, proteggere i docenti stessi, che, in qualità di soggetti autorizzati al trattamento, hanno responsabilità precise e possono incorrere in conseguenze disciplinari e penali se non rispettano le regole. Questo strumento, quindi, non ha solo una funzione normativa e organizzativa, ma assume anche un ruolo di **supporto professionale**, poiché accompagna i docenti nelle diverse situazioni operative quotidiane.

Il contesto normativo in cui si inserisce il manuale è caratterizzato da un'evoluzione costante. Il GDPR, entrato in vigore nel 2018, ha rappresentato una vera e propria svolta nella gestione dei dati personali, introducendo principi innovativi come la "responsabilizzazione" del titolare e del responsabile del trattamento, la valutazione del rischio, il concetto di privacy by design e privacy by default. Nel settore scolastico, queste innovazioni hanno avuto un impatto notevole: si è reso necessario rivedere procedure consolidate, aggiornare la modulistica, introdurre sistemi informatici più sicuri e formare in modo specifico tutto il personale.

A differenza di altri contesti lavorativi, la scuola presenta peculiarità che rendono la gestione della privacy particolarmente complessa. In primo luogo, la presenza di minori implica un'attenzione maggiore, poiché i dati dei bambini e degli adolescenti sono considerati particolarmente sensibili. Inoltre, le attività didattiche e organizzative della scuola spesso richiedono la raccolta e il trattamento di informazioni che vanno ben oltre i semplici dati anagrafici: si pensi ai certificati medici per gli esoneri dalle attività motorie, ai piani educativi personalizzati per gli studenti con bisogni educativi speciali, alle autorizzazioni per le gite scolastiche o per la pubblicazione di fotografie sul sito istituzionale.

Il manuale nasce, quindi, come strumento pratico, ma anche culturale: non si tratta solo di rispettare formalmente degli adempimenti, bensì di diffondere tra i docenti una vera e propria **cultura della protezione dei dati**, che si traduca in comportamenti corretti, consapevoli e responsabili. In quest'ottica, la privacy non è un ostacolo all'attività educativa, ma un valore aggiunto, poiché contribuisce a creare un clima di fiducia tra scuola e famiglie e a rafforzare il ruolo educativo dell'istituzione.

Un altro elemento fondamentale è l'attenzione alla dimensione digitale. Negli ultimi anni, la scuola ha conosciuto un'accelerazione nell'uso delle tecnologie informatiche, specialmente durante il periodo della didattica a distanza. L'utilizzo di piattaforme online, registri elettronici, ambienti digitali di apprendimento ha ampliato le possibilità di insegnamento, ma al tempo stesso ha moltiplicato i rischi legati alla sicurezza dei dati. In questo scenario, il manuale si propone di fornire ai docenti indicazioni operative concrete per ridurre tali rischi, attraverso l'adozione di buone pratiche digitali.

Infine, è importante sottolineare che il manuale non è un documento statico. Al contrario, deve essere inteso come uno strumento **dinamico**, aggiornato periodicamente alla luce delle evoluzioni normative, tecnologiche e organizzative. Il suo scopo non è solo quello di imporre regole, ma anche di stimolare nei docenti una riflessione critica sul proprio operato, invitandoli a segnalare eventuali criticità e a contribuire al miglioramento continuo delle procedure.

In sintesi, le finalità del manuale possono essere così riassunte:

1. Fornire un quadro chiaro e aggiornato delle norme in materia di protezione dei dati applicabili in ambito scolastico.
2. Definire i comportamenti corretti che ogni docente deve adottare nel trattamento dei dati personali.
3. Prevenire violazioni della privacy e ridurre i rischi legati a un uso improprio delle informazioni.
4. Rafforzare la collaborazione tra docenti, famiglie e studenti, basata sulla fiducia e sul rispetto reciproco.
5. Accompagnare i docenti in un percorso di crescita professionale, che li renda consapevoli non solo dei propri doveri, ma anche del valore etico della tutela della persona.

In conclusione, questo primo capitolo mette in luce come il manuale non sia un mero adempimento burocratico, ma uno strumento indispensabile per garantire una scuola più sicura, più trasparente e più attenta alla dignità di ciascun individuo.

Capitolo 2 – Figure e ruoli nel trattamento dei dati personali

Nel contesto scolastico, la corretta gestione dei dati personali non può prescindere da una chiara definizione delle figure coinvolte e dei rispettivi ruoli. La normativa europea e nazionale in materia di protezione dei dati individua infatti precisi soggetti responsabili del trattamento, ciascuno con compiti e responsabilità ben delineate. Comprendere questi ruoli è essenziale per i docenti, poiché permette loro di collocare il proprio operato all'interno di una cornice giuridica e organizzativa chiara, evitando confusioni che potrebbero tradursi in errori o violazioni della privacy.

1. Il Titolare del trattamento

Il **Titolare del trattamento** è il soggetto – persona fisica o giuridica, pubblica o privata – che decide le finalità e i mezzi del trattamento dei dati personali. Nelle scuole statali italiane, questa figura coincide con il **Dirigente Scolastico**. È infatti il dirigente che, in quanto rappresentante legale dell'istituto, stabilisce le modalità con cui i dati devono essere trattati e le finalità per cui essi vengono raccolti.

Il Titolare ha il compito di:

- garantire che i trattamenti avvengano nel rispetto della normativa vigente;
- designare eventuali **Responsabili del trattamento**;
- fornire istruzioni precise agli **Autorizzati** (docenti e personale scolastico);
- vigilare sul corretto utilizzo dei dati, adottando le necessarie misure di sicurezza;
- informare gli interessati (alunni, famiglie, personale) attraverso informative chiare e complete.

Per i docenti, riconoscere il ruolo del Dirigente come Titolare significa comprendere che non agiscono mai in autonomia assoluta nella gestione dei dati: ogni trattamento deve essere effettuato in conformità alle istruzioni ricevute e agli strumenti predisposti dalla scuola.

2. Il Responsabile del trattamento

Il **Responsabile del trattamento** è la persona fisica o giuridica che, sulla base di un contratto o di un atto formale, tratta dati personali per conto del Titolare. Nelle scuole, questa figura è spesso individuata nel **Direttore dei Servizi Generali e Amministrativi (DSGA)**, oppure in consulenti esterni che si occupano di servizi informatici, piattaforme digitali, gestione di archivi elettronici.

Il Responsabile ha l'obbligo di:

- rispettare le istruzioni del Titolare;
- adottare misure tecniche e organizzative adeguate alla protezione dei dati;
- supportare il Titolare nell'adempimento di obblighi specifici, come la gestione delle violazioni di dati (data breach);
- garantire che il personale autorizzato sia adeguatamente formato e consapevole delle proprie responsabilità.

Per i docenti, la presenza del Responsabile significa avere un referente a cui rivolgersi per problematiche tecniche o organizzative relative al trattamento dei dati, soprattutto quando si utilizzano strumenti informatici.

3. Gli Autorizzati al trattamento

Gli **Autorizzati al trattamento** sono i membri del personale scolastico (docenti, collaboratori scolastici, amministrativi) che, per svolgere le proprie mansioni, hanno accesso ai dati personali degli alunni e delle loro famiglie. Essi operano **sotto l'autorità del Titolare**, che li designa formalmente e fornisce loro specifiche istruzioni.

Gli Autorizzati hanno il compito di:

- trattare i dati solo per le finalità strettamente legate alla propria funzione;
- rispettare le regole interne dell'istituto;
- mantenere la riservatezza anche al termine del rapporto di lavoro o dell'incarico;
- segnalare immediatamente eventuali anomalie o violazioni della sicurezza.

Per i docenti, essere Autorizzati al trattamento significa comprendere che l'accesso alle informazioni non è un privilegio, ma una **responsabilità**. Ogni dato di cui vengono a conoscenza deve essere custodito con attenzione, evitando comunicazioni indebite o usi personali.

4. Altre figure collegate

Oltre a queste figure principali, esistono altri soggetti rilevanti:

- **Gli interessati**: sono gli alunni, le famiglie e il personale scolastico i cui dati vengono trattati. Essi hanno il diritto di essere informati e di esercitare i propri diritti (accesso, rettifica, cancellazione, limitazione, opposizione).
- **Il Responsabile della Protezione dei Dati (RPD o DPO)**: figura introdotta dal GDPR, obbligatoria per le scuole. È un consulente indipendente che supporta l'istituto nella gestione della privacy, vigila sul rispetto delle norme e funge da punto di contatto con l'Autorità Garante.
- **Gli organi collegiali** (consigli di classe, collegio docenti, GLI, ecc.), che possono trattare dati in quanto parte integrante dell'organizzazione scolastica.

5. L'importanza della chiarezza nei ruoli

Spesso i docenti vivono la gestione dei dati come un compito burocratico accessorio rispetto all'attività didattica. Tuttavia, la chiarezza nei ruoli permette di comprendere meglio **chi fa cosa** e di evitare fraintendimenti. Ad esempio, un docente non deve inventarsi procedure di conservazione dei dati, ma seguire quelle predisposte dal Titolare e dal Responsabile. Allo stesso modo, non deve assumere decisioni autonome sulla diffusione di informazioni (ad esempio pubblicare foto online), ma attenersi alle regole comuni.

La responsabilità condivisa, ma distinta nei ruoli, consente alla scuola di funzionare come una squadra: ogni figura ha compiti specifici, ma tutti contribuiscono alla tutela della privacy.

6. Conclusione

Il capitolo sui ruoli mette in evidenza che la protezione dei dati in ambito scolastico non è questione di singoli, ma di **organizzazione complessiva**. Il docente, in quanto Autorizzato, deve collocarsi in questo quadro con consapevolezza, riconoscendo la propria responsabilità e al tempo stesso contando sul supporto delle altre figure. Solo così sarà possibile coniugare l'attività didattica con il rispetto delle norme e la salvaguardia dei diritti degli studenti e delle loro famiglie.

Capitolo 3 – I principi fondamentali del GDPR e la loro applicazione nella scuola

Il **Regolamento Europeo 2016/679 (GDPR)** rappresenta il pilastro normativo in materia di protezione dei dati personali. Esso definisce i principi generali che devono guidare qualsiasi trattamento di dati, sia in ambito pubblico che privato. Nella scuola, tali principi assumono una rilevanza particolare: l'istituto, infatti, gestisce quotidianamente dati di minori e delle loro famiglie, quindi soggetti che godono di una tutela rafforzata. Per questo motivo, ogni docente è chiamato a comprendere in profondità i principi del GDPR e a tradurli in prassi concrete nella vita scolastica quotidiana.

1. Liceità, correttezza e trasparenza

Il primo principio stabilisce che i dati possono essere trattati solo se esiste una **base giuridica legittima**. Nella scuola, questa base è spesso rappresentata dall'adempimento di un obbligo legale (ad esempio la tenuta dei registri) o dall'esecuzione di un compito di interesse pubblico (come l'organizzazione delle attività didattiche). In alcuni casi è richiesto anche il **consenso esplicito** delle famiglie, ad esempio per la pubblicazione di immagini o per attività non strettamente obbligatorie.

La correttezza implica che i dati siano trattati con rispetto per la persona, senza abusi né eccessi. La trasparenza significa che gli interessati – studenti e genitori – devono essere informati in modo chiaro su come vengono utilizzati i loro dati: per questo motivo le scuole sono tenute a fornire **informative dettagliate**, pubblicate anche sul sito istituzionale.

2. Limitazione della finalità

I dati devono essere raccolti solo per **scopi specifici e legittimi**. In ambito scolastico, le finalità possono essere:

- la gestione didattica (registri, valutazioni, assenze);
- la gestione organizzativa (gite scolastiche, elezioni degli organi collegiali);
- l'inclusione (piani personalizzati per studenti con bisogni educativi speciali);
- la sicurezza e la salute (certificati medici, esoneri).

Il docente non può utilizzare i dati raccolti per finalità diverse: ad esempio, non è lecito diffondere a terzi informazioni sulle condizioni di salute di uno studente o condividere dati su gruppi privati non autorizzati (come chat WhatsApp).

3. Minimizzazione dei dati

Un altro principio fondamentale è quello della **minimizzazione**: raccogliere e trattare solo i dati strettamente necessari. Ciò significa che, se per organizzare una visita didattica è sufficiente un elenco con i nomi degli studenti e i recapiti di emergenza, non è lecito richiedere ulteriori informazioni non pertinenti.

Per i docenti, questo principio si traduce in una domanda da porsi costantemente: *"Questi dati mi servono davvero per svolgere la mia attività?"*. In caso di dubbio, è preferibile limitarsi a ciò che è indispensabile.

4. Esattezza e aggiornamento

I dati devono essere **corretti e aggiornati**. Nel contesto scolastico, ciò significa che i docenti devono segnalare eventuali incongruenze o errori riscontrati (ad esempio nei registri elettronici o nelle anagrafiche) e collaborare con la segreteria affinché le informazioni siano sempre affidabili.

Un dato non aggiornato può avere conseguenze rilevanti: basti pensare a un numero telefonico errato che impedisce di contattare tempestivamente la famiglia in caso di emergenza.

5. Limitazione della conservazione

I dati non possono essere conservati oltre il tempo necessario al raggiungimento delle finalità per cui sono stati raccolti. Nella scuola, alcuni documenti devono essere archiviati per legge (ad esempio registri d'esame o verbali), mentre altri possono essere eliminati dopo un certo periodo.

Per i docenti, questo significa evitare di trattenere copie personali di registri, elenchi o documenti sensibili una volta concluso l'anno scolastico. Tutto il materiale deve essere restituito o distrutto in modo sicuro, secondo le procedure dell'istituto.

6. Integrità e riservatezza

Il principio di **integrità e riservatezza** impone di proteggere i dati da accessi non autorizzati, perdite o divulgazioni indebite. Per questo motivo, i docenti devono:

- custodire con cura registri e documenti cartacei;
- utilizzare password personali e sicure per i registri elettronici;
- evitare di lasciare computer o tablet incustoditi;
- non condividere documenti sensibili tramite canali non ufficiali.

L'uso della posta elettronica personale o di chat private per comunicazioni sensibili è una delle violazioni più frequenti: occorre ricordare che i soli strumenti autorizzati sono quelli istituzionali (email della scuola, registro elettronico, piattaforme approvate).

7. Responsabilizzazione (accountability)

Il GDPR introduce anche il principio di **responsabilizzazione**: non basta rispettare le regole, ma occorre dimostrarlo. Questo significa che ogni docente deve essere in grado di spiegare come gestisce i dati e di provare di aver adottato comportamenti corretti.

Nella pratica, ciò comporta:

- l'uso esclusivo delle credenziali personali;
- la firma dei documenti che attestano l'avvenuta formazione in materia di privacy;
- la partecipazione agli aggiornamenti organizzati dalla scuola;
- la collaborazione con il Dirigente e il DPO in caso di verifiche o controlli.

8. Privacy by design e by default

Infine, due concetti chiave del GDPR:

- **Privacy by design**: significa che la protezione dei dati deve essere integrata fin dalla progettazione di qualsiasi attività o progetto scolastico. Ad esempio, quando si organizza un nuovo modulo di didattica digitale, bisogna prevedere subito come gestire la privacy degli studenti.
- **Privacy by default**: significa che, per impostazione predefinita, devono essere raccolti e trattati solo i dati strettamente necessari. Ad esempio, nelle piattaforme digitali devono essere attivate solo le funzioni indispensabili, evitando di rendere pubbliche informazioni che non servono.

Conclusione

L'applicazione dei principi del GDPR nella scuola non è un mero obbligo formale, ma un elemento centrale della professionalità docente. Ogni principio si traduce in scelte operative quotidiane: dall'uso corretto del registro elettronico alla gestione delle comunicazioni con le famiglie, dalla custodia dei documenti cartacei alla selezione delle informazioni realmente necessarie. Solo interiorizzando questi principi e trasformandoli in buone pratiche sarà possibile garantire una scuola rispettosa dei diritti, sicura e trasparente.

Capitolo 4 – Tipologie di dati trattati dai docenti: comuni, particolari, giudiziari

Uno degli aspetti più rilevanti della protezione dei dati personali è la consapevolezza della **natura dei dati trattati**. Il GDPR distingue chiaramente tra diverse categorie di informazioni e attribuisce a ciascuna di esse un livello di protezione diverso. Per i docenti, conoscere queste tipologie non è un dettaglio tecnico, ma una necessità operativa: solo comprendendo la differenza tra dati comuni, particolari e giudiziari è possibile adottare le corrette cautele e rispettare le procedure imposte dall'istituto scolastico.

1. Dati comuni

I **dati comuni** sono le informazioni di base che identificano un individuo senza rivelare aspetti sensibili della sua vita personale. Nella scuola, rientrano in questa categoria:

- nome, cognome, data e luogo di nascita;
- indirizzi di residenza e recapiti telefonici;
- informazioni anagrafiche e scolastiche (classe frequentata, sezione, orario scolastico);
- valutazioni scolastiche, voti, giudizi periodici;
- presenze e assenze;
- partecipazione a commissioni, gruppi di lavoro, elezioni scolastiche.

Questi dati, pur essendo considerati meno delicati rispetto ai sensibili, devono comunque essere trattati con **liceità e riservatezza**. Ad esempio, i voti di una verifica non possono essere resi pubblici a tutta la classe in modo da esporre gli studenti al giudizio dei compagni, ma devono essere comunicati individualmente attraverso strumenti ufficiali (registro elettronico o colloqui).

Un errore frequente riguarda la gestione dei documenti cartacei, come gli elenchi degli alunni per le gite scolastiche: tali documenti non devono circolare liberamente, ma essere custoditi in modo da evitare che persone non autorizzate possano prenderne visione.

2. Dati particolari (o sensibili)

Il GDPR definisce "**categorie particolari di dati**" quelli che rivelano aspetti intimi della persona e che, se divulgati, possono comportare discriminazioni o danni gravi. In ambito scolastico, i docenti trattano quotidianamente diversi dati sensibili, tra cui:

- informazioni sanitarie: certificati medici per esoneri da educazione fisica, attestazioni di patologie croniche (asma, diabete, allergie, cardiopatie);
- disabilità e bisogni educativi speciali: piani educativi individualizzati (PEI), piani didattici personalizzati (PDP), documenti BES e DSA;
- convinzioni religiose: scelta di avvalersi o meno dell'insegnamento della religione cattolica, richieste di giustificazione per festività religiose non cattoliche, regimi alimentari particolari;
- convinzioni sindacali o filosofiche: partecipazione a iniziative o assemblee interne;
- eventuali informazioni sullo stato psico-emotivo degli studenti, rilevabili da colloqui, relazioni o osservazioni didattiche.

Questi dati richiedono un livello di protezione **più elevato**. Devono essere custoditi in contenitori chiusi a chiave se cartacei, oppure in archivi elettronici protetti da password robuste. Non devono mai essere divulgati se non a personale autorizzato e solo per le finalità strettamente connesse alla didattica e all'inclusione scolastica.

Un esempio pratico: se un alunno soffre di una grave allergia alimentare, l'informazione deve essere condivisa con i docenti e con il personale della mensa, ma non resa pubblica a tutta la classe.

3. Dati giudiziari

Un'ulteriore categoria, spesso sottovalutata, è quella dei **dati giudiziari**, ossia le informazioni che rivelano procedimenti giudiziari in corso o provvedimenti di natura penale. Nella scuola, queste situazioni possono emergere in diversi contesti:

- provvedimenti disciplinari che abbiano riflessi di carattere giudiziario;
- segnalazioni da parte dei servizi sociali o del tribunale dei minori;
- situazioni particolari che riguardano l'affidamento o la potestà genitoriale.

Per i docenti, l'accesso a tali dati è limitato e avviene solo se strettamente necessario per lo svolgimento della funzione educativa. L'uso improprio di informazioni giudiziarie può avere conseguenze gravissime, sia per lo studente interessato sia per l'operatore che viola la riservatezza.

4. Dati impliciti e indiretti

Oltre alle categorie classiche, è importante considerare anche i **dati indiretti** che emergono da attività apparentemente innocue. Un tema di italiano scritto da uno studente può rivelare informazioni delicate sulla sua vita familiare o sulla sua salute; una fotografia scattata durante una gita può rivelare la partecipazione di un minore la cui immagine non doveva essere diffusa.

Per questo motivo, i docenti devono essere particolarmente attenti a come gestiscono non solo i dati ufficiali, ma anche quelli che emergono incidentalmente dall'attività didattica.

5. Il principio di necessità

La distinzione tra le diverse tipologie di dati si collega direttamente al **principio di necessità**: il docente deve accedere e trattare solo i dati che gli servono realmente. Non è necessario conoscere lo stato di salute di uno studente se non incide sulla propria attività didattica; allo stesso modo, non è opportuno conservare documenti che contengono informazioni non pertinenti.

6. Rischi legati alla gestione impropria

Un errore nella classificazione dei dati può comportare conseguenze serie. Ad esempio, se un docente considera un dato sanitario come se fosse un dato comune, potrebbe archiviarlo senza le dovute cautele, esponendolo al rischio di diffusione indebita. Inoltre, la condivisione impropria di dati particolari o giudiziari può dar luogo a sanzioni disciplinari, amministrative e persino penali.

7. Conclusione

La gestione dei dati personali da parte dei docenti non si limita all'utilizzo del registro elettronico o alla compilazione dei verbali: riguarda un insieme vasto e complesso di informazioni che spaziano dagli aspetti didattici a quelli sanitari e sociali. La consapevolezza della tipologia di dati trattati è il primo passo per garantire un trattamento corretto e sicuro. Solo distinguendo chiaramente tra dati comuni, particolari e giudiziari sarà possibile adottare le misure adeguate e rispettare la dignità e la riservatezza di ciascun alunno e delle loro famiglie.

Capitolo 5 – Regole operative per i docenti nella gestione dei dati

Le regole operative costituiscono la parte più concreta e applicativa del manuale: rappresentano cioè le linee guida che ogni docente deve seguire quotidianamente per garantire il corretto trattamento dei dati personali degli alunni, delle famiglie e del personale scolastico. Se i principi del GDPR (liceità, minimizzazione, sicurezza) costituiscono il quadro teorico, le regole operative traducono quei principi in azioni pratiche, semplici e verificabili. In questo capitolo analizziamo dunque quali comportamenti devono adottare i docenti per assicurare che la gestione delle informazioni sia conforme alla normativa e rispettosa della dignità delle persone.

---

1. Uso degli strumenti ufficiali

La regola fondamentale è utilizzare **esclusivamente i canali e gli strumenti ufficiali** messi a disposizione dalla scuola. Ciò significa che:

- le comunicazioni scuola-famiglia devono avvenire tramite registro elettronico, email istituzionale o piattaforme autorizzate;
- non è lecito utilizzare account personali di posta elettronica, chat private (WhatsApp, Telegram) o social network per la trasmissione di dati sensibili;
- le piattaforme di didattica digitale integrata devono essere quelle approvate dall'istituto e non sistemi privati scelti autonomamente dal docente.

Questo aspetto, apparentemente banale, è in realtà una delle criticità più frequenti: molti docenti, per praticità, tendono a comunicare con i genitori tramite canali informali. Tuttavia, questa prassi espone al rischio di violazioni della privacy e può compromettere la sicurezza dei dati.

---

2. Custodia dei registri

Il registro, cartaceo o elettronico, è lo strumento principale del docente, ma anche uno dei più delicati. Contiene infatti dati personali e sensibili relativi ad assenze, voti, note disciplinari, osservazioni sul comportamento.

- I **registri cartacei** devono essere custoditi in armadi chiusi a chiave quando non utilizzati, e mai lasciati incustoditi in aula.
- I **registri elettronici** devono essere utilizzati solo tramite credenziali personali, che non vanno mai condivise con colleghi, alunni o genitori.
- In caso di smarrimento delle credenziali o sospetto accesso da parte di terzi, il docente deve immediatamente informare il Dirigente Scolastico o il DSGA.

---

3. Trattamento dei documenti cartacei

Molte attività scolastiche richiedono ancora l'uso di documenti cartacei (certificati medici, autorizzazioni per uscite, relazioni didattiche). Tali documenti devono essere:

- acquisiti solo se strettamente necessari;
- custoditi in buste chiuse o contenitori sicuri;
- restituiti agli uffici competenti dopo l'uso;
- distrutti in maniera sicura quando non più necessari (ad esempio mediante distruggi-documenti).

Un errore frequente è conservare nel proprio cassetto documenti contenenti dati sensibili anche dopo che non servono più: questa prassi va evitata.

---

4. Comunicazioni scuola-famiglia

Le comunicazioni con le famiglie sono un aspetto centrale dell'attività docente, ma richiedono grande attenzione:

- i colloqui devono rispettare la riservatezza, evitando di trattare dati sensibili alla presenza di altre persone;
- le comunicazioni scritte devono avvenire tramite i canali ufficiali;
- in nessun caso i dati di un alunno devono essere comunicati a genitori di altri studenti;
- le autorizzazioni per gite, uscite o attività extracurricolari devono essere raccolte su moduli ufficiali predisposti dalla scuola.

---

5. Diffusione di immagini e materiali

La pubblicazione di fotografie, video o lavori prodotti dagli alunni richiede sempre il **consenso scritto** delle famiglie. Anche in presenza di consenso, occorre comunque adottare cautele:

- evitare di associare le immagini a dati identificativi (nome, cognome, classe);
- pubblicare solo su canali istituzionali (sito della scuola, bacheche ufficiali);
- accertarsi che non vengano diffusi indirettamente dati sensibili (ad esempio, una foto che mostra un alunno in condizione di disabilità senza adeguata contestualizzazione).

---

6. Gestione dei dati sensibili

Quando il docente viene a conoscenza di informazioni relative a condizioni di salute, situazioni familiari delicate o appartenenze religiose, deve adottare una regola aurea: **parlare solo con chi è autorizzato a sapere**.

- È lecito condividere con il consiglio di classe informazioni utili per l'inclusione scolastica.
- Non è lecito diffondere tali informazioni ad altri studenti o genitori.
- Qualsiasi documento contenente dati sensibili deve essere trattato con massima riservatezza e non lasciato incustodito.

---

7. Obbligo di segnalazione

Se un docente si accorge di una possibile violazione dei dati (ad esempio documenti smarriti, accessi non autorizzati, email inviate a destinatari sbagliati), ha l'obbligo di segnalarlo immediatamente al Dirigente o al DSGA. Non si deve tentare di nascondere l'errore: la normativa prevede procedure specifiche per gestire i cosiddetti **data breach**, e la collaborazione di chi ha rilevato l'anomalia è fondamentale.

---

8. Segretezza e continuità

La responsabilità del docente non termina con la fine dell'anno scolastico o con il trasferimento in altra scuola. La regola del **segreto professionale** permane anche dopo la cessazione dell'incarico: le informazioni conosciute in qualità di autorizzato devono rimanere riservate, e la loro diffusione indebita può costituire reato (art. 326 c.p., rivelazione di segreto d'ufficio).

---

9. Conclusione

Le regole operative non devono essere vissute come un ostacolo burocratico, ma come strumenti di tutela reciproca: tutelano gli alunni, che vedono rispettata la propria privacy, e tutelano i docenti, che si muovono all'interno di un quadro chiaro e sicuro. In un'epoca in cui la quantità di dati trattati è enorme e il rischio di violazioni sempre più alto, l'adozione di regole semplici ma rigorose rappresenta l'unico modo per conciliare efficacia didattica e rispetto della legge.

Capitolo 6 – Buone pratiche digitali e sicurezza informatica

La scuola contemporanea è sempre più legata al mondo digitale. Registri elettronici, piattaforme di didattica digitale, comunicazioni online e gestione di archivi informatici fanno ormai parte integrante dell'attività quotidiana dei docenti. Questa evoluzione ha portato indubbi vantaggi in termini di efficienza, rapidità e trasparenza, ma ha introdotto anche nuove sfide legate alla sicurezza dei dati personali. Un uso superficiale o non consapevole degli strumenti digitali può infatti esporre alunni, famiglie e personale scolastico a rischi di violazione della privacy. Per questo motivo, è fondamentale che i docenti adottino **buone pratiche digitali** e sviluppino una sensibilità specifica in materia di sicurezza informatica.

---

1. Gestione delle credenziali di accesso

Ogni docente dispone di credenziali personali per accedere al registro elettronico e alle piattaforme didattiche. Queste credenziali rappresentano la "chiave" di accesso a un enorme patrimonio di dati personali. È quindi essenziale:

- non condividere mai le password con colleghi, studenti o genitori;
- utilizzare password complesse, composte da lettere maiuscole, minuscole, numeri e caratteri speciali;
- modificare periodicamente le password, evitando di riutilizzare sempre le stesse;
- non annotare le credenziali su fogli lasciati incustoditi o su dispositivi non protetti.

Una prassi pericolosa, ma purtroppo diffusa, è quella di utilizzare password semplici e facilmente intuibili, come la propria data di nascita: questo espone a rischi elevati di accesso non autorizzato.

---

2. Accesso sicuro ai sistemi

I docenti devono accedere al registro elettronico e alle piattaforme digitali solo da **dispositivi sicuri**. Ciò significa:

- evitare l'uso di computer pubblici o di reti Wi-Fi non protette;
- attivare sistemi di blocco automatico dello schermo quando il dispositivo non è utilizzato;
- effettuare sempre il logout al termine della sessione di lavoro.

Un computer lasciato acceso e incustodito in sala professori può diventare una fonte di rischio: chiunque potrebbe consultare i dati sensibili degli studenti.

---

3. Protezione dei dispositivi personali

Molti docenti utilizzano i propri computer o smartphone per attività legate alla scuola. In questo caso, occorre adottare ulteriori cautele:

- installare software antivirus e mantenerlo aggiornato;
- attivare sistemi di cifratura e protezione dei file contenenti dati scolastici;
- non salvare in memoria permanente documenti contenenti dati sensibili, ma conservarli solo per il tempo strettamente necessario;
- sincronizzare i dispositivi solo con servizi cloud approvati dall'istituto, evitando l'uso di piattaforme personali non autorizzate.

---

4. Uso della posta elettronica

La posta elettronica è uno strumento fondamentale, ma anche uno dei canali più vulnerabili. I docenti devono:

- utilizzare esclusivamente l'email istituzionale per le comunicazioni scolastiche;
- prestare attenzione agli allegati ricevuti, evitando di aprire file da mittenti sconosciuti;
- verificare con cura l'indirizzo dei destinatari prima di inviare documenti, per evitare errori che possano esporre dati personali;
- non inoltrare comunicazioni contenenti dati sensibili a liste di distribuzione generiche.

Un errore banale, come inviare un file con i dati di una classe a un destinatario sbagliato, può costituire un **data breach** con conseguenze rilevanti.

---

5. Piattaforme di didattica digitale integrata (DDI/DAD)

Le piattaforme utilizzate per la didattica a distanza o mista devono essere quelle approvate dall'istituto. L'uso di strumenti non autorizzati (ad esempio videoconferenze organizzate tramite account personali) può esporre a rischi di violazione. Durante le lezioni online è necessario:

- garantire che l'accesso sia riservato solo agli studenti autorizzati;
- non registrare le lezioni se non strettamente necessario e previo consenso;
- evitare di condividere sullo schermo documenti contenenti dati sensibili non pertinenti alla lezione;
- ricordare agli studenti e alle famiglie le regole di comportamento digitale, compreso il divieto di diffondere immagini o registrazioni senza autorizzazione.

---

6. Archiviazione e conservazione dei dati digitali

Gli archivi digitali devono essere gestiti con la stessa attenzione di quelli cartacei:

- i documenti devono essere conservati in cartelle protette da password;
- le copie devono essere limitate allo stretto necessario;
- i backup devono essere effettuati su supporti sicuri e autorizzati dall'istituto;
- i file obsoleti devono essere cancellati in modo definitivo, evitando di lasciarli nel cestino del computer.

---

7. Attenzione alle trappole digitali

I docenti devono sviluppare consapevolezza rispetto ai rischi più diffusi nel mondo digitale:

- **phishing**: email apparentemente attendibili che mirano a carpire credenziali;
- **malware**: programmi dannosi che si installano tramite allegati infetti;
- **social engineering**: tentativi di ottenere informazioni tramite inganno o manipolazione.

La regola d'oro è: *se un messaggio suscita anche il minimo dubbio, non aprire allegati né cliccare su link, ma contattare il responsabile tecnico dell'istituto.*

---

8. Cultura della sicurezza digitale

Le buone pratiche digitali non sono solo un insieme di regole tecniche, ma rappresentano una **cultura della responsabilità**. Ogni docente deve essere consapevole che il proprio comportamento ha un impatto diretto sulla sicurezza dell'intera comunità scolastica. Una disattenzione individuale può compromettere la protezione dei dati di centinaia di studenti.

---

9. Conclusione

La sicurezza informatica non è un compito riservato agli esperti tecnici, ma una responsabilità condivisa da tutti i docenti. Adottare buone pratiche digitali significa proteggere non solo i dati, ma anche la credibilità della scuola e la fiducia delle famiglie. In un'epoca in cui la dimensione digitale è parte integrante della didattica, la professionalità del docente si misura anche nella sua capacità di gestire con consapevolezza e rigore gli strumenti informatici.

Capitolo 7 – Responsabilità disciplinari, civili e penali dei docenti

Il trattamento dei dati personali in ambito scolastico non è un'attività priva di conseguenze. Ogni docente, in qualità di soggetto autorizzato, è titolare di responsabilità precise e non può sottrarsi agli obblighi derivanti dalla normativa vigente. Queste responsabilità si articolano su tre livelli – **disciplinare, civile e penale** – e costituiscono un insieme di doveri a cui il docente deve attenersi per garantire il rispetto della legge e la tutela dei diritti degli studenti e delle loro famiglie.

---

1. La responsabilità disciplinare

La responsabilità disciplinare riguarda la violazione delle regole interne della scuola e delle istruzioni impartite dal Titolare del trattamento (il Dirigente scolastico). Quando un docente non segue le procedure indicate nel manuale o contravviene alle disposizioni organizzative, può incorrere in provvedimenti disciplinari.

Esempi di condotte che possono comportare sanzioni disciplinari:

- lasciare incustoditi registri cartacei o elettronici contenenti dati personali;
- diffondere a terzi informazioni riservate sugli studenti senza autorizzazione;
- utilizzare strumenti non ufficiali (chat private, email personali) per trattare dati sensibili;
- non rispettare le regole sulla custodia dei documenti o sulla gestione delle password.

Le sanzioni disciplinari possono variare in base alla gravità della violazione: da un richiamo scritto fino alla sospensione dal servizio, nei casi più gravi. L'obiettivo non è punire, ma richiamare il docente al rispetto di regole che tutelano l'intera comunità scolastica.

---

2. La responsabilità civile

Oltre agli aspetti disciplinari, il docente risponde anche civilmente di eventuali danni arrecati a terzi a causa di una gestione scorretta dei dati. Se, ad esempio, la diffusione indebita di informazioni sensibili provoca un danno morale o materiale allo studente o alla sua famiglia, l'istituto scolastico (in quanto Titolare) può essere chiamato a risarcire. In questi casi, però, il docente che ha commesso la violazione può essere ritenuto personalmente responsabile e subire azioni di rivalsa da parte della scuola.

La responsabilità civile, quindi, comporta l'obbligo di risarcire il danno prodotto, che può consistere in:

- danno patrimoniale (ad esempio costi sostenuti dalla famiglia per tutelare i propri diritti);
- danno non patrimoniale (lesione della dignità, stress, discriminazione subita).

Questa prospettiva evidenzia come la gestione corretta dei dati non sia solo un dovere professionale, ma anche una tutela per il docente stesso, che evita di incorrere in conseguenze economiche personali.

---

3. La responsabilità penale

Il livello più grave di responsabilità è quello **penale**, che scatta quando la condotta del docente configura un vero e proprio reato. In questo ambito, due norme sono particolarmente rilevanti:

- **Art. 326 del Codice Penale**: punisce la *rivelazione e utilizzazione di segreti d'ufficio*. Se un docente divulga informazioni riservate di cui è venuto a conoscenza in virtù del proprio incarico, può essere perseguito penalmente.
- **Art. 167 del Codice Privacy**: punisce il trattamento illecito dei dati personali, quando esso provoca un danno all'interessato o comporta un vantaggio ingiusto per chi lo commette.

Esempi concreti di condotte penalmente rilevanti:

- divulgare pubblicamente le condizioni di salute di uno studente;
- pubblicare online, senza consenso, immagini che rivelano dati sensibili;
- accedere ai registri elettronici di altre classi senza motivazione didattica;
- utilizzare i dati acquisiti in ambito scolastico per fini personali o esterni alla scuola.

Le sanzioni penali possono consistere in ammende o persino in pene detentive, a seconda della gravità del fatto.

---

4. La responsabilità condivisa

È importante ricordare che la responsabilità dei docenti non si esaurisce nella propria condotta individuale, ma si inserisce in un sistema di responsabilità condivise. Il Dirigente Scolastico, in qualità di Titolare del trattamento, ha la responsabilità primaria; tuttavia, gli autorizzati che non rispettano le istruzioni ricevute rispondono personalmente delle violazioni commesse.

In pratica, se un docente agisce al di fuori delle regole impartite dall'istituto, non può giustificarsi dicendo di aver agito "per il bene degli studenti": la legge richiede che ogni trattamento avvenga solo nei limiti delle finalità stabilite e con le modalità previste.

---

5. La prevenzione come strumento di tutela

La miglior difesa contro i rischi disciplinari, civili e penali è la **prevenzione**. Ciò significa adottare comportamenti rigorosi e consapevoli:

- rispettare sempre le regole del manuale e le istruzioni del Dirigente;
- mantenere alta l'attenzione sulla riservatezza, evitando leggerezze;
- partecipare alle attività di formazione sulla privacy;
- segnalare tempestivamente eventuali anomalie o sospetti di violazione.

Agendo in questo modo, il docente non solo riduce i rischi legali, ma rafforza anche la propria credibilità professionale e il rapporto di fiducia con studenti e famiglie.

---

6. Conclusione

Le responsabilità disciplinari, civili e penali dimostrano quanto la gestione dei dati non sia un aspetto marginale della professione docente, ma un pilastro fondamentale. Essere insegnanti significa anche saper custodire informazioni delicate, trattarle con rispetto e responsabilità, e comprendere che dietro ogni dato c'è una persona con diritti che non possono essere violati. In questo senso, la consapevolezza delle conseguenze giuridiche non deve generare paura, ma favorire un comportamento prudente e rispettoso, che rende la scuola un luogo più sicuro e affidabile.

Capitolo 8 – Checklist operativa e linee guida pratiche

Dopo aver analizzato i principi, i ruoli, le regole e le responsabilità, è necessario tradurre tutta questa cornice normativa e teorica in strumenti concreti di lavoro. I docenti, infatti, hanno bisogno non solo di conoscere cosa dice la legge, ma soprattutto di sapere **come agire** nella vita quotidiana della scuola. Per questo motivo, il manuale si conclude con una **checklist operativa** e con un insieme di linee guida pratiche, che fungono da vademecum immediato e semplificato.

La checklist non sostituisce le norme né le regole interne dell'istituto, ma le integra, diventando una sorta di "mappa di controllo" che aiuta i docenti a verificare se stanno operando correttamente. È uno strumento utile anche per l'autoformazione: ripercorrere periodicamente i punti della lista consente di individuare eventuali errori o abitudini scorrette e di correggerle in tempo.

---

1. Checklist quotidiana

Ogni giorno, durante l'attività scolastica, il docente deve porsi alcune domande di verifica:

- Ho effettuato l'accesso al registro elettronico con le mie credenziali personali e in modo sicuro?
- Ho custodito adeguatamente i registri cartacei, evitando di lasciarli incustoditi?
- Le comunicazioni con le famiglie sono avvenute esclusivamente tramite canali ufficiali (registro, email istituzionale, colloqui)?
- Ho evitato di trattare dati sensibili davanti ad altri alunni o persone non autorizzate?
- Ho lasciato il computer o il tablet incustodito e connesso al registro?

Questa serie di controlli rapidi permette di ridurre al minimo gli errori più comuni e di rafforzare le buone abitudini.

---

2. Checklist periodica

Con cadenza mensile o trimestrale, è opportuno fare una revisione più approfondita:

- Ho cambiato la password dei miei account istituzionali?

- Ho eliminato o archiviato in modo sicuro i documenti cartacei non più necessari?
- Ho cancellato in modo definitivo i file obsoleti contenenti dati sensibili?
- Ho seguito eventuali aggiornamenti o corsi di formazione offerti dalla scuola sulla protezione dei dati?
- Sono a conoscenza di eventuali aggiornamenti delle linee guida interne?

Questa verifica periodica aiuta il docente a mantenere alta l'attenzione e a non accumulare pratiche scorrette.

---

3. Checklist per la gestione dei dati sensibili

Quando si trattano dati particolarmente delicati, come quelli sanitari o relativi a situazioni familiari, il docente deve verificare:

- È davvero necessario acquisire questo dato per svolgere la mia funzione?
- Il dato è custodito in un contenitore sicuro o in un file protetto da password?
- La condivisione con altri colleghi è strettamente indispensabile?
- È stato acquisito il consenso esplicito delle famiglie, se richiesto (ad esempio per immagini o pubblicazioni)?

Seguire questi passaggi riduce i rischi di violazioni e garantisce maggiore tutela per gli studenti.

---

4. Checklist in caso di emergenza o violazione (data breach)

Può capitare che si verifichi un errore o una perdita di dati. In questi casi, il docente deve agire senza esitazione:

- Ho informato immediatamente il Dirigente Scolastico o il DSGA?
- Ho descritto con precisione l'accaduto, indicando quali dati sono stati coinvolti?
- Ho seguito le istruzioni fornite dall'istituto per gestire l'incidente?

Agire tempestivamente non significa ammettere una colpa, ma collaborare alla tutela della comunità scolastica.

---

5. Linee guida pratiche per i docenti

Oltre alla checklist, è utile sintetizzare alcune regole operative in forma di linee guida:

- **Non improvvisare procedure**: attenersi sempre alle istruzioni ricevute dal Dirigente o dal Responsabile.
- **Non accumulare dati**: trattare solo ciò che serve, evitando archivi personali paralleli.
- **Non sottovalutare i dettagli**: anche un elenco con nomi e numeri di telefono è un dato personale da proteggere.
- **Non usare strumenti privati**: evitare email personali, chat e cloud non autorizzati.
- **Comunicare con trasparenza**: informare sempre gli interessati su come vengono trattati i loro dati.
- **Mantenere il segreto professionale**: ciò che viene appreso in qualità di docente deve restare riservato anche dopo la cessazione del rapporto.

---

6. La checklist come strumento educativo

Un aspetto spesso trascurato è che la checklist non è utile solo per i docenti, ma può diventare un **modello educativo per gli studenti**. Mostrare attenzione alla riservatezza, custodire con cura i documenti, usare correttamente le piattaforme digitali: tutto ciò costituisce un esempio di cittadinanza digitale responsabile. In questo modo, il docente non si limita a rispettare la legge, ma trasmette agli studenti un valore fondamentale: il rispetto della privacy come diritto umano e come regola di convivenza civile.

---

7. Conclusione

La checklist operativa e le linee guida pratiche rappresentano la sintesi del manuale. Non sostituiscono la conoscenza approfondita delle norme, ma forniscono uno strumento immediato, semplice e applicabile in qualsiasi momento. Ogni docente dovrebbe tenerne una copia a disposizione, consultarla regolarmente e interiorizzarne i punti principali. In questo modo, la protezione dei dati non sarà percepita come un obbligo burocratico, ma come una parte integrante della professionalità docente, capace di rafforzare la fiducia tra scuola, famiglie e studenti.

Il Dirigente Scolastico

Prof. Emanuele Ridulfo

Firmato digitalmente da:
Prof. RIDULFO EMANUELE
18/09/2025 13:55:17