ISTRUZIONI OPERATIVE INCARICATI DEL TRATTAMENTO

PREMESSA

Il presente documento contiene le istruzioni operative per gli incaricati del trattamento dei dati personali della Scuola, conformemente al Regolamento (Ue) 2016/679 (GDPR).
I docenti, il personale amministrativo, il personale tecnico, il personale ausiliario, i consulenti ed in generale tutte le persone autorizzate ad accedere ai dati personali e preposte allo svolgimento delle operazioni di trattamento relativa ai dati, devono ispirarsi a un principio generale di diligenza e correttezza.
Ogni utilizzo dei dati in possesso della Scuola diverso da finalità istituzionali, è espressamente vietato.
Di seguito vengono esposte le regole comportamentali da seguire per evitare e prevenire condotte che anche inconsapevolmente potrebbero comportare rischi alla sicurezza del sistema informativo e all'immagine della Scuola.

DEFINIZIONI

Secondo l'articolo 4 del Regolamento (Ue) 2016/679 (GDPR), si definisce:

- **Dato personale**: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- **Trattamento**: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
- **Violazione dei dati personali**: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

ADEMPIMENTI

Ciascun incaricato del trattamento deve:

- rispettare i principi generali del Regolamento (Ue) 2016/679 (GDPR), con particolare riferimento alla liceità e correttezza del proprio agire, all'obbligo di procedere alla raccolta e alla registrazione dei dati per scopi determinati, espliciti e legittimi;
- rispettare l'obbligo di riservatezza e segretezza e conseguentemente il divieto di comunicazione e diffusione dei dati trattati nel corso dell'incarico svolto;
- utilizzare i dati, cui abbia accesso, solamente per finalità compatibili all'esecuzione delle proprie mansioni o dei compiti affidati, per cui è autorizzato ad accedere alle informazioni e ad utilizzare gli strumenti messi a disposizione dall'istituto scolastico;
- rispettare le misure di sicurezza idonee adottate dalla Scuola, atte a salvaguardare la riservatezza e l'integrità dei dati;
- segnalare eventuali malfunzionamenti di strumenti elettronici, perdite di dati o esigenze (sia di natura organizzativa, sia tecnica), che possano migliorare lo svolgimento delle operazioni

affidate;
- accedere ai dati strettamente necessari all'esercizio delle proprie funzioni e competenze;
- in caso di interruzione del lavoro, anche temporanea, verificare che i dati trattati non siano accessibili a terzi non autorizzati;
- mantenere riservate le proprie credenziali di autenticazione;
- svolgere le attività previste dai trattamenti secondo le direttive del responsabile del trattamento dei dati; non modificare i trattamenti esistenti o introdurre nuovi trattamenti senza l'esplicita autorizzazione del responsabile del trattamento dei dati;
- rispettare e far rispettare le norme di sicurezza per la protezione dei dati personali;
- informare il responsabile in caso di incidente di sicurezza che coinvolga dati particolari e non;
- raccogliere, registrare e conservare i dati presenti negli atti e documenti contenuti nei fascicoli di archiviazione e nei supporti informatici avendo cura che l'accesso ad essi sia possibile solo ai soggetti autorizzati;
- eseguire qualsiasi altra operazione di trattamento nei limiti delle proprie mansioni e nel rispetto delle norme di legge.

ISTRUZIONI PER IL PERSONALE

Gestione raccolta dati

- identificazione dell'interessato: al momento della raccolta dei dati personali o del rilascio di documenti, qualora sia necessario individuare l'identità del soggetto richiedente, è obbligatorio richiedere un documento di identità o di riconoscimento, al fine di verificare la identità e di procedere correttamente alla raccolta e alla registrazione delle informazioni;
- verifica del controllo dell'esattezza del dato e della corretta digitazione: al momento della registrazione dei dati raccolti direttamente o indirettamente, occorre prestare attenzione al corretto inserimento dei dati identificativi e degli altri dati riferiti all'interessato, al fine di evitare errori, che potrebbero generare problemi nella corretta gestione dell'anagrafica e nello svolgimento delle operazioni, che caratterizzano il processo di trattamento;

Norme logistiche per l'accesso fisico ai locali

I locali ove sono custoditi i dati personali (ed in particolare categorie di dati particolari), devono essere soggetti a controllo e a verifica, al fine di evitare che durante l'orario di lavoro possano essere conosciuti o accessibili da parte di soggetti non autorizzati. Si raccomanda, in caso di allontanamento dal proprio ufficio o dalla propria postazione di lavoro, di adottare tutte le accortezze e precauzioni al fine di impedire l'accesso fisico a chi non sia legittimato, soprattutto se esterno all'istituto scolastico. Laddove si esegue il trattamento di Dati Personali, deve essere possibile archiviare i documenti cartacei in luogo ed i supporti rimovibili contenenti tali dati in luogo sicuro ove le porte degli uffici ed almeno un armadio per ufficio devono essere dotati di serratura con chiave. Al termine dell'orario lavorativo, ove la dinamica delle attività ed il numero di occupanti lo consentano, è necessario chiudere sempre a chiave gli uffici nei quali vengono svolti trattamenti di dati personali.

Rilevazione presenze

Ove possibile, si raccomanda di dotarsi di un servizio di rilevazione delle presenze e di un servizio di reception / sorveglianza. In questo caso, ogni incaricato è tenuto ad utilizzare sempre i sistemi di rilevazione presenze disponibili, allo scopo di segnalare la propria presenza e legittimare le attività in corso di svolgimento.

Gestione strumenti informatici

Come principio generale, sia i dispositivi di memorizzazione del proprio PC sia le unità di rete, devono contenere informazioni strettamente legate alle attività scolastiche e non possono essere utilizzate per scopi diversi (immagini, video e documenti personali).

Ciascun incaricato è responsabile del corretto utilizzo e della custodia degli strumenti elettronici in dotazione (a titolo esemplificativo personal computer, periferiche, lettori di smart card). Si devono adottare le misure di sicurezza per la tutela della riservatezza, consistenti nell'evitare che l'accesso ai dati possa avvenire da parte di soggetti estranei o non specificamente autorizzati.

Per la gestione della sessione di lavoro sul PC, è necessario che:

- al termine delle ore di servizio, il PC deve essere spento, a meno che non stia svolgendo elaborazioni particolari. In tal caso gli uffici debbono tassativamente essere chiusi a chiave;
- se l'incaricato si assenta momentaneamente dalla propria postazione deve accertarsi che l'eventuale sessione di lavoro aperta non sia accessibile da altre persone. Deve chiudere la sessione di lavoro sul PC facendo logout, oppure in alternativa avere attivo un salvaschermo (**screen- saver**) protetto dalle credenziali di autenticazione;
- Relativamente all'utilizzo dello screen-saver, occorre osservare le seguenti regole:
  - Non deve mai essere disattivato;
  - Il suo avvio automatico deve essere previsto non oltre i primi 5 minuti di inattività del PC;
  - Deve essere messo in funzione manualmente ogni volta che si lascia il PC incustodito ed acceso;
- Quando si esegue la stampa di un documento contenente dati personali, in particolare una stampante condivisa, occorre ritirare tempestivamente i documenti stampati per evitare l'accesso a soggetti non abilitati al trattamento.

Gestione username e password

L'accesso al PC, sia esso collegato in rete o meno, è protetto da un sistema di autenticazione che richiede all'incaricato di inserire sulla videata di accesso all'elaboratore un codice utente (**username**) ed una parola chiave (**password**). L'adozione ed il corretto utilizzo della combinazione username / password è fondamentale per il corretto utilizzo del PC, in quanto:

- tutela l'utilizzatore ed in generale l'Azienda da accessi illeciti, atti di vandalismo e, in generale, violazioni e danneggiamenti del proprio patrimonio informativo;
- tutela l'Incaricato da false imputazioni, garantendo che nessuno possa operare a suo nome e che, con il suo profilo (ossia con le sue user id e password) solo lui possa svolgere determinate azioni;
- è necessario per gestire correttamente gli accessi a risorse condivise.

Ciascun incaricato deve scegliere le password in base ai seguenti criteri:

- devono essere lunghe almeno otto caratteri;
- non devono fare riferimento ad informazioni agevolmente riconducibili ai soggetti utilizzatori o ai loro familiari;
- devono contenere una combinazione di numeri e/o segni speciali, lettere, maiuscole e minuscole;
- non deve essere uguali alle precedenti.

Per la corretta gestione della password è necessario:

- almeno ogni 4 mesi è obbligatorio cambiare la password;
- ogni password ricevuta va modificata al primo utilizzo;
- la password venga conservata in un luogo sicuro;
- non rivelare o condividere la password con i colleghi di lavoro, familiari e amici, soprattutto attraverso il telefono;
- non utilizzare la funzione, offerta da alcuni software, di salvare automaticamente la password per successivi utilizzi delle applicazioni.

Installazione di hardware e software

L'installazione di hardware e software, nonché la modifica dei parametri di configurazione, possono essere eseguiti solamente dalle persone del Servizio Informatico su mandato del Responsabile del trattamento per i Sistemi Elettronici.
Si raccomanda agli utenti dei PC di rispettare i seguenti divieti:

- Non utilizzare sul PC dispositivi personali, quali lettori dispositivi di memorizzazione dei dati;
- Non installare sistemi per connessione esterne (es : modem, wifi); tali connessioni, aggirando i sistemi preposti alla sicurezza della rete scolastica, aumentano sensibilmente i rischi di intrusioni e di attacchi dall'esterno;
- Non installare programmi, anche in versione demo. In particolare, è vietata l'installazione di giochi, programmi in prova (shareware), programmi gratuiti (freeware), programmi pirata, e in generale tutti i software non autorizzati dal Servizio Informatico;
- Non modificare i parametri di configurazione del proprio PC senza espressa autorizzazione e senza il supporto di personale tecnico qualificato.

Si ricorda che normalmente la condivisione di aree e di risorse del proprio PC è vietata. Può essere autorizzata dal Servizio Informatico, solo in casi eccezionali e solo per il tempo strettamente necessario allo svolgimento delle attività di lavoro. In questi casi devono essere adottate password di lettura e scrittura e la condivisione deve operare solo su singole directory del PC, e non sull'intero disco rigido.

Gestione posta elettronica

Il servizio di posta elettronica viene fornito per permettere la comunicazione con soggetti terzi interni ed esterni per le finalità della Scuola e in stretta connessione con l'effettiva attività del dipendente che utilizza tale funzionalità.
Al fine di non compromettere la sicurezza della Scuola e di prevenire conseguenze legali a carico della stessa, bisogna adottare le seguenti norme comportamentali:

- Se si ricevono mail da destinatari sconosciuti contenenti file di qualsiasi tipo, procedere alla loro immediata eliminazione;
- È fatto divieto di utilizzare le caselle di posta elettronica per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail list, salvo diversa ed esplicita autorizzazione;
- La casella di posta elettronica assegnata deve essere mantenuta in ordine, cancellando i documenti inutili specialmente se contengono allegati ingombranti come dimensione.
- Nell'ipotesi in cui la e-mail debba essere utilizzata per la trasmissione di dati particolari, si raccomanda di prestare attenzione a che:
  - l'indirizzo del destinatario sia stato correttamente digitato,

- l’oggetto del messaggio non contenga direttamente il riferimento a stati, fatti o qualità idonei a rivelare dati di natura sensibile;
- nel corpo del messaggio sia presente un’intestazione standardizzata in cui si avverta della confidenzialità/riservatezza del messaggio;

Gestione protezione da virus informatici

Per prevenire eventuali danneggiamenti al software causati dalla presenza o dall’azione di programmi virus informatici, su ogni elaboratore della Scuola è stato installato un software antivirus che si aggiorna automaticamente all’ultima versione disponibile.
L’antivirus non deve mai essere disattivato o sostituito con altro antivirus non ufficialmente fornito.
Nel caso il programma antivirus installato sul proprio PC riscontri la presenza di un virus, oppure si sospetti la presenza di un virus non rilevato dal programma antivirus è necessario darne immediatamente segnalazione al responsabile del Servizio Informatico.
Si raccomanda di non scaricare e né tantomeno aprire file provenienti via e-mail da mittenti sconosciuti. Tali file, possono essere portatori di virus e compromettere la funzionalità del PC, l’integrità dei dati in essa contenuti e soprattutto l’integrità dei sistemi collegati al PC stesso.

Formazione

Il personale scolastico deve seguire una formazione su ingegneria sociale, phishing, tecnologie cloud, attacchi ransomware e simili.

Gestione Registro Elettronico

Il software di **ARGO**, adottato dalla Scuola, permette di interagire in tempo reale con tutti i dati che la scuola vuole rendere disponibili al docente scolastico, alla segreteria, ai docenti e alle famiglie attraverso un qualsiasi accesso a internet. Esso consente di operare tutte le attività attinenti la gestione del registro (di classe, personale del docente e registro delle conoscenze/abilità) in un ambiente unico, senza mai dovere uscire dalla finestra di lavoro. Tutte le funzioni necessarie alle attività del docente, previo inserimento di password personale a cui sono collegate le autorizzazioni ad operare nel proprio ambito di pertinenza, sono immediatamente disponibili. La scuola non deve ricaricare o trasferire i dati su nuovi archivi e non deve creare files diversi da quelli esistenti, deve semplicemente collegarsi al portale. Per i dipendenti abilitati è possibile visualizzare i propri dati contabili, di servizio e delle assenze.
La sicurezza e la privacy, nonché le diverse tipologie di dati consultabili in funzione delle prerogative di accesso (Docente, Personale amministrativo, Personale tecnico, famiglia etc.), sono controllati mediante chiavi d'accesso individuali, generate da un’apposita procedura interna e comunicabili ai destinatari in modalità sicura. Le richieste provenienti dalle utenze sono indirizzate ai server del sistema, che fanno da intermediari dei flussi dati informatici e garantiscono protezione e affidabilità funzionale. Infine, i dati immessi e quelli ricevuti vengono cifrati durante il loro intero percorso telematico al fine di impedirne qualsiasi manipolazione
I profili di accesso ai servizi gestiti sono i seguenti.:
Docente, Docente Coordinatore, Dirigente, Assistente/Educatore, Personale Ata, Genitore/Alunno

ISTRUZIONI SPECIFICHE PER I DOCENTI

L'attività di trattamento dati all'interno della Scuola da parte dei Docenti si esplica principalmente attraverso le seguenti modalità: gestione del registro elettronico, comunicazioni all'interno della scuola, comunicazioni scuola-famiglia.
La gestione del Registro elettronico segue una procedura di sicurezza e di autorizzazioni guidata dal software, per cui il docente deve seguire le seguenti regole:

- la password deve essere conservata in un luogo sicuro (es: chiavetta USB protetta)
- non rilevare o condividere la password di accesso personale comunicata dal sistema
- in caso di utilizzo di files locali per l'inserimento di dati nel registro, provvedere alla loro cancellazione una volta terminato il trasferimento
- se si prevede l'utilizzo di un supporto mobile come una chiavetta USB, questo deve essere criptato e protetto da password, e tenuto al sicuro

Per le comunicazioni all'interno della scuola è preferibile che il docente abbia un'e-mail istituzionale collegata al servizio di posta elettronica della Scuola per la quale osservi le seguenti regole:

- consultare periodicamente la casella di posta elettronica (si può inserire un "alert" nel registro)
- se si ricevono mail da destinatari sconosciuti contenenti file di qualsiasi tipo, procedere alla loro immediata eliminazione;
- è fatto divieto di utilizzare le caselle di posta elettronica per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail list, salvo diversa ed esplicita autorizzazione;
- la casella di posta elettronica assegnata deve essere mantenuta in ordine, cancellando i documenti inutili specialmente se contengono allegati ingombranti come dimensione.

Per le comunicazioni scuola – famiglia, i docenti si avvalgono dell'ausilio della segreteria per eventuali richieste di colloqui personali ed in generale devono assicurarsi che nell'ambito dei colloqui sia assicurata la riservatezza dei dati relativi agli alunni interessati, escludendo l'eventualità di fornire informazioni riservate ad estranei.

L'**inserimento dati** di eventuali **certificazioni** ex legge 104/92 o **diagnosi** di Dsa o altri Bes avviene in un apposito campo che è visibile soltanto ai docenti del consiglio di classe; questi, tuttavia, dovranno prestare attenzione a non accedere a tali campi quando la schermata viene visualizzata (a mezzo Lim o altro monitor) anche dagli studenti o da soggetti esterni che non abbiano la necessità di conoscere lo stato di salute del ragazzo in questione.

E' vivamente sconsigliato per i docenti attivare gruppi Whatsapp con gli studenti, al di fuori di ogni tipo di controllo dei dati trattati da parte dell'Istituto scolastico.

ISTRUZIONI PER L'USO DEGLI STRUMENTI "NON ELETTRONICI"

Per "non elettronici" si intendono, per le Scuole, i documenti cartacei. I documenti cartacei contenenti dati particolari relativi allo stato di salute e/o giudiziari devono essere protetti in appositi armadi dotati di chiavi. Tutti i documenti contenenti dati particolari (ex dati sensibili) o giudiziari che si ritiene debbano essere eliminati devono essere distrutti e non gettati nei cestini.
Per proteggere i dati personali è opportuno evitare il deposito di documenti di qualsiasi genere negli ambienti di transito o pubblici (corridoi o sale riunioni), come pure l'abbandono in vista sulle scrivanie quando ci si debba assentare dal proprio posto di lavoro. Nel caso di dati particolari relativi allo stato di salute e/o giudiziari, il rispetto di queste norme è obbligatorio.

Distruzione delle copie cartacee

Coloro che sono preposti alla duplicazione di documentazione (con stampanti o fotocopiatrici o altre periferiche) ovvero che utilizzando strumenti per la riproduzione cartacea di documenti digitali, sono tenuti a procedere alla relativa distruzione del supporto, qualora si verifichino errori o la riproduzione non sia corretta, evitando di riutilizzare i fogli, salva l'ipotesi di uso esclusivamente personale per eventuali appunti o brutte copie, da distruggere immediatamente quando non più necessarie.

Misure di sicurezza

Il trattamento sicuro di documenti contenenti Dati Personali richiede la presenza di misure di sicurezza con le quali l'incaricato possa interagire ed una serie di accorgimenti direttamente gestibili dall'incaricato stesso. In particolare, si richiede:
- la presenza e l'uso tassativo di armadi e cassetti dotati di serratura adeguata;
- la presenza e l'uso tassativo, ove si richieda la distruzione di documenti contenenti dati particolari (ex dati sensibili) e giudiziari, di un tritadocumenti.

Prescrizioni per gli incaricati

L'incaricato deve attenersi alle seguenti prescrizioni:
- in nessun caso è concesso l'accesso a documentazione contenente Dati Personali per motivi non dettati da esigenze di lavoro strettamente connesse ai trattamenti dichiarati, autorizzati e tutelati dal Titolare;
- la documentazione contenente Dati Personali che, per ragioni di praticità operativa, risiede sulle scrivanie degli incaricati, deve comunque essere rimossa al termine dell'orario di lavoro;
- i documenti contenenti dati personali, non devono essere lasciati incustoditi in un ambiente non controllato (ad es. a seguito della stampa dei documenti su stampante di rete);
- il numero di copie di documenti contenenti Dati Personali deve essere strettamente funzionale alle esigenze di lavoro;
- cassetti ed armadi contenenti documentazione riservata debbono tassativamente essere chiusi a chiave fuori dell'orario di lavoro;
- la distruzione di documenti contenenti Dati Personali deve essere operata, ove possibile,

direttamente dal personale incaricato;
• ove non siano disponibili strumenti per la distruzione dei documenti (trita documenti), o il volume di questi sia tale da imporre il ricorso al servizio di macero, il personale incaricato che avvia al macero la documentazione è tenuto a confezionare tale documentazione in modo che il pacco risulti anonimo e solido;
• è severamente vietato utilizzare documenti contenenti Dati personali, dati particolari (ex dati sensibili) o giudiziari come carta da riciclo o da appunti.

ISTRUZIONI PER ADDETTI ALLA MANUTENZIONE

Le seguenti istruzioni devono essere osservate dai preposti in qualità di addetti alla gestione o manutenzione che trattano dati di titolarità per i quali è nominato un responsabile del trattamento nonché dagli addetti di ditte specializzate che svolgano interventi tecnici di gestione e manutenzione degli strumenti elettronici:
• effettuare operazioni di manutenzione e supporto per verifica corretto funzionamento (monitoraggio e diagnostica) su flussi dei dati;
• gestire le credenziali di autenticazione dei soggetti incaricati del trattamento su indicazione dell'Amministratore di sistema;
• gestire i profili di autorizzazione degli incaricati al trattamento dei dati su indicazione dell'Amministratore di sistema;
• provvedere alla disattivazione/variazione delle utenze, ivi compreso l'account di posta elettronica, assegnate al personale cessato dal servizio o che abbia modificato il proprio ambito di trattamento, su richiesta specifica dei responsabili del personale e su indicazione dell'Amministratore di sistema;
• custodire la documentazione cartacea, prodotta nello svolgimento dei propri compiti istituzionali;
L'accesso agli addetti alla gestione e manutenzione è consentito unicamente ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere alle operazioni di manutenzione dei programmi o del sistema informatico.
A ciascun addetto alla manutenzione, previa sottoscrizione di apposito atto per accettazione, è pertanto consentito eseguire le operazioni strettamente necessarie a tali scopi e/o richieste dal titolare, secondo le seguenti istruzioni operative:
• nel caso in cui sia necessario effettuare stampe di prova per controllare il funzionamento di stampanti o per verificare il funzionamento di strumenti o programmi installati, non utilizzare files già esistenti ma creare files di prova.
• nel caso si renda strettamente necessario accedere a files contenenti dati (ad esempio per il recupero di un testo) limitare l'accesso ai dati per il tempo strettamente necessario all'assolvimento delle operazioni di manutenzione.
• per effettuare operazioni di manutenzione sui database aziendali che prevedano la raccolta e la conservazione dei dati, tali dati dovranno essere custoditi in modo tale da non essere accessibili da soggetti non autorizzati.
• devono inoltre essere adottate le misure di sicurezza adeguate previste dal Regolamento UE 2016/679 in materia di protezione dei dati personali;
• è necessario informare al più presto il titolare o il responsabile del trattamento qualora si dovessero riscontrare malfunzionamenti o non conformità.
• tutti i dati personali contenuti nei data base devono essere protetti da password;
• nel caso in cui sia necessario accedere ai dati attraverso gli strumenti elettronici in dotazione agli incaricati, attenersi alle seguenti indicazioni:

- in presenza dell'incaricato, far digitare la password dall'incaricato stesso evitando di venirne a conoscenza;

- in assenza dell'incaricato rivolgersi alla persona individuata dall'incaricato quale proprio fiduciario il quale provvederà all'inserimento della password.

• nei casi in cui sia necessario accedere ai dati personali attraverso il server, rivolgersi all'amministratore di sistema o provvedere, in collaborazione con l'amministratore di sistema stesso, alla creazione di credenziali di autenticazione da utilizzarsi esclusivamente per l'accesso da parte degli addetti alla manutenzione/gestione dei sistemi informatici;
• l'amministratore di sistema ha facoltà, in qualunque momento di controllare e verificare l'operato degli addetti alla manutenzione;
• qualora si renda necessario prelevare apparecchiature elettroniche per effettuare attività di ripristino o interventi di manutenzione che comportino il reset di password precedentemente individuate, la nuova password di accesso sarà comunicata all'incaricato il quale provvederà a cambiarla al termine delle operazioni di manutenzione;
• l'accesso al sistema informatico da parte degli addetti alla manutenzione/gestione del sistema è consentito unicamente previo inserimento di password e ID;
• è assolutamente vietato comunicare o diffondere i dati personali di qualsiasi natura provenienti dai database gestiti dalla scuola, se non previa espressa comunicazione scritta;
• nel caso in cui ci si avvalga di soggetti esterni per interventi specialistici che comportino trattamento di dati personali deve essere rilasciata una dichiarazione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni in materia di misure adeguate di sicurezza

OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PROTEZIONE DATI PERSONALI

È obbligatorio attenersi alle disposizioni in materia di protezione dati personali e di misure adeguate di sicurezza, ai sensi del GDPR 2016/679.

AGGIORNAMENTO E REVISIONE

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni alle presenti istruzioni, le proposte verranno esaminate dalla Direzione.
Le presenti istruzioni sono soggette a revisione con frequenza annuale.

L'Aquila, 16 gennaio 2020

La Direzione

REGOLE GENERALI

STUDENTI E FAMIGLIE INFORMATE

Tutte le scuole – sia quelle pubbliche, sia quelle private - hanno l'obbligo di far conoscere agli "interessati" (studenti, famiglie, professori, etc.) come vengono trattati i loro dati personali. Devono cioè rendere noto, attraverso un'adeguata informativa, quali dati raccolgono, come li utilizzano e a quale fine.
Le informative in uso presso l'Istituto sono le seguenti:

- Informativa alle famiglie degli alunni sull'uso dei dati personali conferiti all'Istituto
- Informativa autorizzazione all'utilizzo di immagini e video
- Informativa personale interno, a tempo determinato. ed occasionale (Docenti, ATA, Commissari)
- Informativa privacy agli allievi per i servizi a supporto dell'inclusione scolastica
- Informative sul Sito

TRATTAMENTO DEI DATI NELLE ISTITUZIONI SCOLASTICHE PUBBLICHE

Le istituzioni scolastiche pubbliche possono trattare solamente i dati personali necessari al perseguimento di specifiche finalità istituzionali oppure quelli espressamente previsti dalla normativa di settore.

Il D.Lgs. 101/2018 specifica le materie nelle quali si considera **rilevante l'interesse pubblico** nel trattamento dei dati personali che è pertanto ammesso con adeguate misure di garanzia - 25 materie tra le quali: **istruzione e formazione in ambito scolastico, professionale, superiore o universitario.**

E' quindi garantito il principio di liceità del trattamento, altri principi di riferimento per l'applicazione del GDPR nelle scuole sono:

- Limitazione delle finalità:
  l'istituto scolastico tratta dati personali di alunni, genitori, docenti e personale ATA esclusivamente nell'ambito dei propri compiti istituzionali ed è tenuto a gestire e proteggere tali dati secondo quanto specificato dal Regolamento Generale sulla Protezione dei Dati.
- Minimizzazione dei dati:
  i dati richiesti per assolvere ai propri compiti istituzionali o indicati in eventuali informative da sottoporre in casi particolari devono essere minimi rispetto alle finalità per la quale sono richiesti.
  Un esempio è la richiesta della professione dei genitori degli alunni, dato che può rilevare disagio economico o sociale, e che non deve rientrare tra i dati obbligatori per l'iscrizione, ma solo come dato facoltativo *da raccogliere con un'apposita informativa esclusivamente per finalità statistiche.*

Per tali trattamenti, non sono tenute a chiedere il consenso degli studenti o dei genitori.

DATI SENSIBILI E GIUDIZIARI: ALCUNI ESEMPI CONCRETI

- Origini razziali ed etniche: i dati sulle origini razziali ed etniche possono essere trattati dalla scuola per favorire l'integrazione degli alunni stranieri.
- Convinzioni religiose: gli istituti scolastici possono utilizzare i dati sulle convinzioni religiose al fine di garantire la libertà di culto e per la fruizione dell'insegnamento della religione cattolica o delle attività alternative a tale insegnamento.
- Stato di salute: **i** dati idonei a rivelare lo stato di salute possono essere trattati per l'adozione di specifiche misure di sostegno per gli alunni disabili o con disturbi di apprendimento; per la gestione delle assenze per malattia; per l'insegnamento domiciliare e ospedaliero a favore degli alunni affetti da gravi patologie; per la partecipazione alle attività sportive, alle visite guidate e ai viaggi di istruzione.
- Convinzioni politiche: le opinioni politiche possono essere trattate dalla scuola esclusivamente per garantire la costituzione e il funzionamento degli organismi di rappresentanza: ad esempio, le consulte e le associazioni degli studenti e dei genitori.
- Dati di carattere giudiziario: i dati di carattere giudiziario possono essere trattati per assicurare il diritto allo studio anche a soggetti sottoposti a regime di detenzione o di protezione, come i testimoni di giustizia.

Casi concreti:

- Eventuali contenziosi: il trattamento di dati relativi allo stato di salute o giudiziari è previsto anche per tutte le attività connesse ai contenziosi con gli alunni e con le famiglie (reclami, ricorsi, esposti, provvedimenti di tipo disciplinare, ispezioni, citazioni, denunce all'autorità giudiziaria, etc.), e per tutte le attività relative alla difesa in giudizio delle istituzioni scolastiche.
- Alcune categorie di dati personali degli studenti e delle famiglie – come quelli relativi alla salute e giudiziari – devono essere trattate con estrema cautela, nel rispetto di specifiche norme di legge, verificando prima non solo la pertinenza e completezza dei dati, ma anche la loro indispensabilità rispetto alle "finalità di rilevante interesse pubblico" che si intendono perseguire. Un esempio è la busta riservata cartacea proveniente dall'autorità giudiziaria o sanitaria destinata al Dirigente Scolastico che ne prende visione e la custodisce in una cassaforte chiusa a chiave assicurando la riservatezza dei dati comunicati.
- Le scuole hanno la necessità di trattare i dati degli alunni per il perseguimento delle finalità istituzionali. Tuttavia, è necessario che vi sia particolare attenzione al rispetto della privacy fin dal momento in cui l'alunno viene iscritto per la prima volta in quel determinato istituto.
  Per questo motivo il **portale "Iscrizioni on line"** propone alla famiglia che si appresta a iscrivere il proprio figlio un'informativa sulle modalità e sulle finalità del trattamento dei dati. In fase di iscrizione, inoltre, il portale propone alcune domande a cui la famiglia è invitata a rispondere (ad esempio: la presenza di certificazione secondo la legge 104/92, la diagnosi di disturbi specifici dell'apprendimento e altro) e le scuole stesse hanno la possibilità di chiedere alcuni dati alle famiglie per poter procedere con gli adempimenti di avvio di anno scolastico quale, tipicamente, la formazione delle classi. Le finalità delle richieste devono essere esplicitate nel modulo e il loro utilizzo è legittimo soltanto se risponde al principio di pertinenza e non eccedenza. Nella successiva fase di perfezionamento dell'iscrizione, così come per **aggiornamenti** che si rendessero necessari in corso dell'anno scolastico, saranno le famiglie a dover presentare la documentazione a supporto che non può essere trasmessa d'ufficio da scuola a scuola, se non in presenza di un'esplicita richiesta delle famiglie, fermo

restando che la spedizione a mezzo posta ordinaria o elettronica presenta una condizione di maggiore vulnerabilità. Dunque, eventuali **certificazioni** ex legge 104/92 o **diagnosi** di Dsa o altri Bes saranno consegnate brevi manu dalla famiglia ai fini di un'eventuale necessità di docente di sostegno (per gli alunni con disabilità) e per la predisposizione delle misure idonee a garantire i diritti previsti dalle normative vigenti (legge 170/2010 per i disturbi dell'apprendimento e direttiva 27 dicembre 2012, con successive circolari applicative, per gli altri bisogni educativi speciali).Il relativo contenuto potrà essere conosciuto soltanto dal dirigente scolastico, dalla segreteria e dai docenti del consiglio di classe ovvero da eventuali referenti e collaboratori del dirigente e dalle altre figure che sono coinvolte nella gestione di tali studenti (ad esempio, il collaboratore scolastico con mansioni di assistenza alla persona dei disabili). Poiché tutte le scuole utilizzano il registro elettronico, l'**inserimento dati** avviene in un apposito campo che è visibile soltanto ai docenti del consiglio di classe; questi, tuttavia, dovranno prestare attenzione a non accedere a tali campi quando la schermata viene visualizzata (a mezzo Lim o altro monitor) anche dagli studenti o da soggetti esterni che non abbiano la necessità di conoscere lo stato di salute del ragazzo in questione. Si pensi, per esempio, agli educatori di cooperative esterne, i quali non devono accedere ai dati degli alunni della classe: tali figure, infatti, vengono preventivamente informate in merito ai bisogni specifici dello studente a loro assegnato dall'ente locale oppure nelle riunioni per la predisposizione dei piani educativi individualizzati.

- Vi sono, poi, casi di **famiglie** che versano **in situazione di disagio**: sarà cura di chi detiene la responsabilità genitoriale informare adeguatamente la scuola per garantire il rispetto di eventuali misure giudiziarie operanti sul minore. Dal canto suo, il dirigente scolastico fornirà al consiglio di classe le sole informazioni necessarie alla gestione dei rapporti scuola-famiglia e con lo studente, oppure alla corretta predisposizione di un piano didattico personalizzato nei casi in cui si reputi necessario.
- **Accesso ai fondi di solidarietà** : sono sempre più frequenti anche le istanze di accesso a fondi di solidarietà che le scuole, nella loro autonomia, possono istituire per aiutare le famiglie in difficoltà economiche: la concessione di libri o altro materiale didattico in comodato d'uso avviene solitamente secondo un regolamento interno, pubblicato nella sezione "Amministrazione trasparente" del sito web, che prevederà la predisposizione di una graduatoria in base a criteri appositamente individuati. È assolutamente vietato pubblicare i nomi e i cognomi degli studenti che hanno fatto richiesta di accedere al fondo ed è da evitare anche il riferimento mediante le "sole" iniziali: i dati in possesso della scuola (che in questo caso comprendono, solitamente, dati economici desumibili dall'Isee) saranno utilizzati esclusivamente per il completamento della pratica relativa.

DIRITTO DI ACCESSO AI DATI PERSONALI

Anche in ambito scolastico, ogni persona ha diritto di conoscere se sono conservate informazioni che la riguardano, di apprenderne il contenuto, di farle rettificare se erronee, incomplete o non aggiornate. Come da Regolamento Generale sulla Protezione dei Dati (Regolamento UE 679/2016 – RGDP), l'interessato può ottenere la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano; opporsi al trattamento; ottenere la portabilità dei dati; revocare eventuale consenso, ove previsto.
Per esercitare questi diritti è possibile rivolgersi direttamente all'indirizzo indicato nell'informativa oppure presentare un'istanza al Titolare del trattamento (in genere l'istituto scolastico di riferimento) con apposito modulo disponibile sul sito del Garante della Protezione dei Dati Personali.
Diverso è il caso dell'accesso agli atti amministrativi che, infatti, non è regolato dal Codice della privacy, né vigilato dal Garante per la protezione dei dati personali. Come indicato nella legge n. 241 del 1990 (e successive modifiche), spetta alla scuola valutare se esistono i presupposti normativi che permettono di prendere visione e di estrarre copia di documenti amministrativi ai soggetti con un "interesse diretto, concreto e attuale" alla conoscibilità degli atti.
Inoltre il diritto di accesso ai dati e ai documenti detenuti dalla pubblica amministrazione (cosiddetto accesso civico), è consentito nelle forme e nei limiti di cui al d.lgs. n.33 del 2013, come modificato dal d.lgs. n. 97 del 2016.

VIOLAZIONE DELLA PRIVACY

In caso di violazione della privacy - come ad esempio la diffusione sul sito internet della scuola dei dati personali in assenza di una idonea base normativa, oppure il trattamento dei dati senza aver ricevuto una adeguata informativa o senza aver espresso uno specifico e libero consenso, qualora previsto - la persona interessata (studente, genitore, docente), può presentare al Garante un'apposita "segnalazione" o un "reclamo" (più circostanziato rispetto alla semplice segnalazione).

VITA DELLO STUDENTE

ISCRIZIONE A SCUOLE E ASILI

Tutti gli istituti di ogni ordine e grado - sia quelli che aderiscono al sistema di iscrizioni on line predisposto dal Ministero sia quelli che utilizzano moduli cartacei – ma anche gli enti locali eventualmente competenti devono prestare particolare attenzione alle informazioni che richiedono per consentire l'iscrizione scolastica.
I moduli base, ad esempio, possono essere adattati per fornire agli alunni ulteriori servizi secondo il proprio piano dell'offerta formativa (POF), ma non possono includere la richiesta di informazioni personali eccedenti e non rilevanti (ad esempio lo stato di salute dei nonni o la professione dei genitori) per il perseguimento di tale finalità.
Particolare attenzione deve essere prestata inoltre all'eventuale raccolta di dati relativi alla salute. Il trattamento di questi dati, oltre a dover essere espressamente previsto dalla normativa, richiede infatti speciali cautele e può essere effettuato solo se tali dati sono indispensabili per l'attività istituzionale svolta.

TEMI IN CLASSE

Non lede la privacy l'insegnante che assegna ai propri alunni lo svolgimento di temi in classe riguardanti il loro mondo personale o familiare. Nel momento in cui gli elaborati vengono letti in classe – specialmente se riguardano argomenti delicati - è affidata alla sensibilità di ciascun insegnante la capacità di trovare il giusto equilibrio tra le esigenze didattiche e la tutela dei dati personali. Restano comunque validi gli obblighi di riservatezza già previsti per il corpo docente riguardo al segreto d'ufficio e professionale, nonché quelli relativi alla conservazione dei dati personali eventualmente contenuti nei temi degli alunni.

VOTI ED ESAMI

Gli esiti degli scrutini o degli esami di Stato sono pubblici. Le informazioni sul rendimento scolastico sono soggette ad un regime di conoscibilità stabilito dal Ministero dell'Istruzione dell'Università e della Ricerca. È necessario però che, nel pubblicare i voti degli scrutini e degli esami nei tabelloni, l'istituto scolastico eviti di fornire, anche indirettamente, informazioni sulle condizioni di salute degli studenti, o altri dati personali non pertinenti. Il riferimento alle "prove differenziate" sostenute dagli studenti portatori di handicap o con disturbi specifici di apprendimento (DSA), ad esempio, non va inserito nei tabelloni, ma deve essere indicato solamente nell'attestazione da rilasciare allo studente.

COMUNICAZIONI SCOLASTICHE

Il diritto–dovere di informare le famiglie sull'attività e sugli avvenimenti della vita scolastica deve essere sempre bilanciato con l'esigenza di tutelare la personalità dei minori.
È quindi necessario evitare di inserire, nelle circolari e nelle comunicazioni scolastiche non rivolte a specifici destinatari, dati personali che rendano identificabili, ad esempio, gli alunni coinvolti in casi di bullismo o in altre vicende particolarmente delicate.

DISABILITÀ E DISTURBI SPECIFICI DELL'APPRENDIMENTO

Le istituzioni scolastiche devono prestare particolare attenzione a non diffondere, anche per mero errore materiale, dati idonei a rivelare lo stato di salute degli studenti, così da non incorrere in sanzioni amministrative o penali.
Non è consentito, ad esempio, pubblicare on line una circolare contenente i nomi degli studenti portatori di handicap. Occorre fare attenzione anche a chi ha accesso ai nominativi degli allievi con disturbi specifici dell'apprendimento (DSA), limitandone la conoscenza ai soli soggetti legittimati previsti dalla normativa, ad esempio i professori che devono predisporre il piano didattico personalizzato.

GESTIONE DEL SERVIZIO MENSA

Gli enti locaIi che offrono il servizio mensa possono trattare – secondo quanto previsto nei rispettivi regolamenti - i dati sensibili degli alunni indispensabili per la fornitura di pasti nel caso in cui debbano rispondere a particolari richieste delle famiglie legate, ad esempio, a determinati dettami religiosi o a specifiche condizioni di salute. Alcune particolari scelte, infatti (pasti vegetariani o rispondenti a determinati dettami religiosi) possono essere idonee a rivelare le convinzioni (religiose, filosofiche o di altro genere) dei genitori e degli alunni. Nel caso di alunni con intolleranze alimentari occorre una particolare cura nella comunicazione a chi è responsabile nella preparazione dei pasti e chi deve esercitare il controllo dell'assegnazione del pasto al soggetto interessato.

DALLA SCUOLA AL LAVORO

Dall' Art. 96 del D.Lgs. 101/2018, al fine di agevolare l'orientamento, la formazione e l'inserimento professionale, anche all'estero, le istituzioni del sistema nazionale di istruzione, su richiesta degli interessati, possono comunicare o diffondere, anche a privati e per via telematica, dati relativi agli esiti formativi, intermedi e finali, degli studenti e altri dati personali, pertinenti in relazione alle predette finalità e indicati nelle informazioni rese agli interessati con esplicita informativa. I dati possono essere successivamente trattati esclusivamente per tali finalità.

CURRICULUM E IDENTITÀ DIGITALE DELLO STUDENTE

Il **Curriculum Vitae Precompilato per gli Studenti** è una delle novità introdotte dalla Maturità 2019 per migliaia di studenti italiani, la novità è stata introdotta con l'articolo 21 della legge n. 62/2017, gli studenti che sosterranno l'esame di maturità 2019 avranno un Curriculum in formato digitale dove saranno contenute tutte le competenze e le esperienze acquisite dagli studenti nel corso del quinquennio.
E' un nuovo strumento che verrà consegnato agli studenti dopo che avranno completato il ciclo di studio e dopo aver superato la maturità, si tratta di un Curriculum a tutti gli effetti ma in formato digitale dove verranno riportate tutte le competenze acquisite durante il percorso di studi e tutte le esperienze maturate anche al di fuori delle aule, come, ad esempio durante i percorsi di alternanza scuola lavoro.
L'introduzione di questo strumento ha come obiettivo di fornire allo studente una certificazione delle sue competenze acquisite durante il percorso di studi che verranno certificate dal Ministero dell'Istruzione, lo scopo finale è quello di aiutare i giovani nell'ingresso nel mondo del lavoro.
L'introduzione del Curriculum Vitae Precompilato per gli Studenti era stata anticipata ad ottobre 2018 con apposita circolare (circolare 3054 Miur) dove si legge che entro il mese di marzo 2019,

sarebbe stato pubblicato il decreto ministeriale per definire il modello del diploma e del curriculum dello studente.

Il **Curriculum Vitae Precompilato per gli Studenti** conterrà quelle che sono le competenze e le esperienze acquisite dagli studenti durante il percorso di studi, informazioni che saranno inserite sono le seguenti:

- le discipline previste nel percorso di studi e il monte ore complessivo;
- le competenze, conoscenze e abilità anche professionali acquisite;
- i livelli di apprendimento conseguiti nelle prove Invalsi, per ciascuna delle discipline oggetto di rilevazione;
- la certificazione delle abilità di comprensione e uso dell'inglese;
- le attività culturali, artistiche e di pratiche musicali, sportive e di volontariato svolte in ambito extrascolastico;
- attività di alternanza scuola lavoro;
- altre eventuali certificazioni conseguite.

Per il 2019 si parte con il curriculum, limitatamente alla parte "formale", ossia la carriera scolastica degli studenti: con i risultati di tutti e 5 anni, durata degli studi e le ore di alternanza scuola-lavoro.

Mentre a partire dal 2020 queste conoscenze saranno integrate con la parte informale del curriculum relativa alle esperienze di volontariato, le certificazioni linguistiche, le pratiche sportive, gli interessi culturali e le competenze acquisite durante la formazione.

Il tesoro di informazioni sulle competenze che possiedono i giovani sarà, con molta probabilità, depositato sul **Portale Unico dei Dati della Scuola**, che nasce per dare forma concreta al comma 136 della Legge 107 del 2015, la Buona Scuola.

Sul portale, infatti, concepito nell'ottica degli Open Data, si legge che oltre ai bilanci delle scuole, ai dati in forma aggregata dell'anagrafe degli studenti, ai piani dell'offerta formativa, tenendo conto del rispetto della privacy, ci saranno anche i dati del curriculum dello studente e del curriculum del docente.

Con il CV precompilato che la scuola riconosce a chi supera l'esame di stato, gli studenti hanno un ottimo biglietto da visita per uscire dai confini delle aule scolastiche e le imprese hanno un tesoro di competenze a cui attingere: una via che, se percorsa al meglio, potrebbe ridurre la distanza tra domanda e offerta di competenze nel mercato del lavoro.

MONDO CONNESSO E NUOVE TECNOLOGIE

CYBERBULLISMO E ALTRI FENOMENI DI RISCHIO

Gli studenti, anche i più giovani, rappresentano spesso l'avanguardia tecnologica all'interno della scuola, grazie alla loro capacità di utilizzare le opportunità offerte da smartphone, tablet e altri strumenti che consentono la connessione costante in rete. Tuttavia alla capacità tecnologica non corrisponde spesso eguale maturità nel comprendere la necessità di difendere i propri diritti e quelli di altre persone, a partire dagli stessi compagni di studio. I giovani devono essere consapevoli che le proprie azioni in rete possono produrre effetti negativi anche nella vita reale e per un tempo indefinito. Troppi ragazzi, insultati, discriminati, vittime di cyberbulli, soffrono, possono essere costretti a cambiare scuola o, nei casi più tragici, arrivare al suicidio. È quindi estremamente importante prestare attenzione in caso si notino comportamenti anomali e fastidiosi su un social network, su sistemi di messaggistica istantanea (come Whatsapp, Snapchat, Skype, Messenger, etc.) o su siti che garantiscono comunicazioni anonime.
Se si è vittime di commenti odiosi, di cyberbullismo, di sexting o di altre ingerenze nella propria vita privata, non bisogna aspettare che la situazione degeneri ulteriormente.
Occorre avvisare subito i compagni, i professori, le famiglie se ci si rende conto che qualcuno è insultato o messo sotto pressione da compagni o da sconosciuti. Si può chiedere al gestore del social network di intervenire contro eventuali abusi o di cancellare testi e immagini inappropriate. In caso di violazioni, è bene segnalare immediatamente il problema all'istituzione scolastica, al Garante della protezione dei dati e alle altre autorità competenti.

SMARTPHONE E TABLET

L'utilizzo di telefoni cellulari, di apparecchi per la registrazione di suoni e immagini è in genere consentito, ma esclusivamente per fini personali, e sempre nel rispetto dei diritti e delle libertà fondamentali delle persone coinvolte (siano essi studenti o professori) in particolare della loro immagine e dignità.
Le istituzioni scolastiche hanno, comunque, la possibilità di regolare o di inibire l'utilizzo di registratori, smartphone, tablet e altri dispositivi elettronici all'interno delle aule o nelle scuole stesse.
Gli studenti e gli altri membri della comunità scolastica, in ogni caso, non possono diffondere o comunicare sistematicamente i dati di altre persone (ad esempio pubblicandoli su Internet) senza averle prima informate adeguatamente e averne ottenuto l'esplicito consenso.
Si deve quindi prestare particolare attenzione prima di caricare immagini e video su blog o social network, oppure di diffonderle attraverso mms o sistemi di messaggistica istantanea. Succede spesso, tra l'altro, che una fotografia inviata a un amico o a un familiare venga poi inoltrata ad altri destinatari, generando involontariamente una comunicazione a catena dei dati personali raccolti. Tale pratica può dar luogo a gravi violazioni del diritto alla riservatezza delle persone riprese, e fare incorrere in sanzioni disciplinari, pecuniarie e in eventuali reati.

IMMAGINI DI RECITE E GITE SCOLASTICHE

Non violano la privacy le riprese video e le fotografie raccolte dai genitori durante le recite, le gite e i saggi scolastici. Le immagini, in questi casi, sono raccolte per fini personali e destinate a un ambito familiare o amicale e non alla diffusione.
Va però prestata particolare attenzione alla eventuale pubblicazione delle medesime immagini su Internet, e sui social network in particolare. In caso di comunicazione sistematica o diffusione diventa infatti necessario, di regola, ottenere il consenso informato delle persone presenti nelle fotografie e nei video.

REGISTRAZIONE DELLA LEZIONE E STRUMENTI COMPENSATIVI

È possibile registrare la lezione esclusivamente per scopi personali, ad esempio per motivi di studio individuale. Per ogni altro utilizzo o eventuale diffusione, anche su Internet, è necessario prima informare adeguatamente le persone coinvolte nella registrazione (professori, studenti…) e ottenere il loro esplicito consenso.
Nell'ambito dell'autonomia scolastica, gli istituti possono decidere di regolamentare diversamente o anche di inibire l'utilizzo di apparecchi in grado di registrare. In ogni caso deve essere sempre garantito il diritto degli studenti con diagnosi DSA (disturbi specifici dell'apprendimento) o altre specifiche patologie di utilizzare tutti gli strumenti compensativi (come il registratore) di volta in volta previsti nei piani didattici personalizzati che li riguardano.

PUBBLICAZIONE ON LINE

PUBBLICITÀ E TRASPARENZA

Le scuole di ogni ordine e grado sono soggette a un regime di pubblicità e trasparenza. È però necessario che gli istituti scolastici prestino particolare attenzione a non rendere accessibili informazioni che dovrebbero restare riservate o a mantenerle on line oltre il tempo consentito, mettendo in questo modo a rischio la privacy e la dignità delle persone a causa di un'errata interpretazione della normativa o per semplice distrazione.
La pubblicazione su Internet di informazioni personali deve essere lecita e non eccedente le finalità istituzionali perseguite. Diversamente, tale diffusione può arrecare non solo un pregiudizio alla riservatezza individuale, ma incrementare anche il rischio che le persone interessate possano subire abusi, come il cosiddetto furto di identità.
Per i documenti non liberamente disponibili on line, restano comunque valide le regole sull'accesso previste in particolare dalla legge n. 241 del 1990 e dal d.lgs. n. 33 del 2013 come modificato dal d.lgs. n. 97 del 2016.

PORTALE UNICO DEI DATI DELLA SCUOLA

Il portale, istituito in seguito all'ultima riforma sulla scuola e al Codice dell'amministrazione digitale, garantirà stabilmente l'accesso e la riutilizzabilità dei dati pubblici del sistema nazionale di istruzione e formazione. I dati raccolti presso l'Anagrafe nazionale degli studenti potranno essere inseriti soltanto in forma aggregata, così da garantire la non identificabilità degli interessati. Tramite il portale - nei limiti e nelle modalità individuate da un apposito decreto ministeriale, sentito il Garante della protezione dei dati - saranno resi accessibili il "curriculum dello studente" e il "curriculum del docente".

GRADUATORIE DEL PERSONALE E SUPPLENZE

Gli istituti scolastici possono pubblicare sui propri siti internet le graduatorie di docenti e personale amministrativo tecnico e ausiliario (ATA) per consentire a chi ambisce a incarichi e supplenze di conoscere la propria posizione e punteggio. Tali liste, giustamente accessibili, devono però contenere solo i dati strettamente necessari all'individuazione del candidato, come il nome, il cognome, il punteggio e la posizione in graduatoria. I dati personali, tra l'altro, non possono rimanere pubblicati on line per un periodo superiore a quello previsto.
È invece illecita, perché eccedente le finalità istituzionali perseguite, la pubblicazione dei numeri di telefono e degli indirizzi privati dei candidati.
Tale diffusione dei contatti personali incrementa, tra l'altro, il rischio di esporre il personale interessato a forme di stalking o eventuale furto di identità.

PAGAMENTO DEL SERVIZIO MENSA

Non si può pubblicare sul sito della scuola, o inserire in bacheca, il nome e cognome degli studenti i cui genitori sono in ritardo nel pagamento della retta o del servizio mensa; né può essere diffuso l'elenco degli studenti, appartenenti a famiglie con reddito minimo o a fasce deboli, che usufruiscono gratuitamente di tale servizio.
Gli avvisi messi on line devono avere carattere generale, mentre alle singole persone ci si deve rivolgere con comunicazioni di carattere individuale.
Il gestore del servizio deve inviare alle famiglie i "bollettini" di pagamento in busta chiusa. Eventuali buoni pasto, tra l'altro, non possono avere colori differenziati in relazione alla fascia di reddito di appartenenza delle famiglie degli studenti beneficiari.
Queste semplici accortezze evitano che soggetti non legittimati possano venire a conoscenza di informazioni idonee a rivelare la situazione economica delle famiglie dei bambini.

SERVIZI DI SCUOLABUS

Gli istituti scolastici e gli Enti locali non possono pubblicare on line, in forma accessibile a chiunque, gli elenchi dei bambini che usufruiscono dei servizi di scuolabus, indicando tra l'altro le rispettive fermate di salita-discesa o altre informazioni sul servizio.
Tale diffusione di dati personali, che tra l'altro può rendere i minori facile preda di eventuali malintenzionati, non può assolutamente essere effettuata o giustificata semplicemente affermando che si sta procedendo in tal senso solo per garantire la massima trasparenza del procedimento amministrativo.

VIDEOSORVEGLIANZA ED ALTRI CASI

VIDEOSORVEGLIANZA CONTRO FURTI E VANDALISMI

È possibile installare un sistema di videosorveglianza negli istituti scolastici quando risulti indispensabile per tutelare l'edificio e i beni scolastici, circoscrivendo le riprese alle sole aree interessate, come ad esempio quelle soggette a furti e atti vandalici. Le telecamere che inquadrano l'interno degli istituti possono essere attivate solo negli orari di chiusura, quindi non in coincidenza con lo svolgimento di attività scolastiche ed extrascolastiche.
Le aree perimetrali esterne, al pari di ogni altro edificio pubblico o privato, possono invece essere oggetto di ripresa, per finalità di sicurezza, anche durante l'orario di apertura dell'istituto scolastico. In questo caso, l'angolo visuale deve essere delimitato in modo da non inquadrare luoghi non strettamente pertinenti l'edificio.
La presenza di telecamere deve sempre essere segnalata da appositi cartelli visibili anche di notte qualora il sistema di videosorveglianza sia attivo in tale orario.

QUESTIONARI PER ATTIVITÀ DI RICERCA

La raccolta di informazioni personali, spesso anche sensibili, per attività di ricerca effettuate da soggetti legittimati attraverso questionari è consentita soltanto se i ragazzi, o i genitori nel caso di minori, sono stati preventivamente informati sulle modalità di trattamento e conservazione dei dati raccolti e sulle misure di sicurezza adottate.
Studenti e genitori devono comunque essere lasciati liberi di non aderire all'iniziativa.

MARKETING E PROMOZIONI COMMERCIALI

Non è possibile utilizzare i dati presenti nell'albo - anche on line - degli istituti scolastici per inviare materiale pubblicitario a casa degli studenti. La conoscibilità a chiunque degli esiti scolastici (ad esempio attraverso il tabellone affisso nella scuola) o di altri dati personali degli studenti non autorizza soggetti terzi a utilizzare tali dati per finalità non previste come, ad esempio, il marketing e la promozione commerciale.

A cura del Responsabile esterno del servizio di protezione dei dati personali ing. Pietro Collevecchio