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