



## ISTITUTO COMPRENSIVO "Guido GOZZANO"

Via Le Maire 24 – 10086 RIVAROLO CANAVESE  
C.F. 92517730013 e-mail [TOIC8AC00D@istruzione.it](mailto:TOIC8AC00D@istruzione.it)  
Sede di Via Le Maire Tel. 0124/424706



---

MISURE DI SICUREZZA TECNICHE E  
ORGANIZZATIVE ADOTTATE, AI SENSI  
DELL'ART. 32 DEL GDPR, DALL'ISTITUTO  
COMPRENSIVO "GUIDO GOZZANO" DI  
RIVAROLO CANAVESE

Ai sensi dell'art. 32 del Regolamento Europeo 2016/679 la Scuola, "tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche", deve implementare e mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio.

Le misure di sicurezza sono costituite dal complesso di misure volte a ridurre al minimo i rischi di distruzione o perdita dei dati, accesso non autorizzato, trattamento non consentito e modifica dei dati.

In questo documento vengono indicate le misure di sicurezza che sono state adottate per la protezione dei dati personali dell'Istituto Comprensivo "G. Gozzano" di Rivarolo Canavese:

- **Misure specifiche per la protezione dei dati**

Misura	Office	Cartaceo
<p><b>Minimizzazione della quantità di dati personali</b></p> <p><i>Descrizione:</i> Misure volte a gestire solo dati personali adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.</p>	<p>La scuola applica il principio di minimizzazione richiedendo solo dati adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.</p>	<p>Vengono trattati i dati degli utenti in moda da rispettare il principio di minimizzazione.</p>
<p><b>Partizionamento dei dati</b></p> <p><i>Descrizione:</i> Misure volte a separare le aree di archiviazione dei dati personali trattati al fine di ridurre la possibilità che i dati possano essere correlati e compromessi, ad esempio attraverso la creazione di cartelle di rete condivise distinte per tipologia di dati personali o l'archiviazione di documentazione cartacea in faldoni o archivi separati.</p>	<p>I dati vengono partizionati in cartelle di rete condivise sul server e in cloud. Inoltre i documenti vengono altresì protocollati con protocollo riservato o ordinario.</p>	<p>I dati vengono suddivisi in faldoni o archivi separati.</p>
<p><b>Cifratura</b></p> <p><i>Descrizione:</i></p>	<p>Il sito della scuola è in https ed inoltre vengono adottate</p>	<p>No</p>

<p><i>Misure volte ad assicurare la riservatezza dei dati personali archiviati (in database, documenti e archivi elettronici, etc.) o trasmessi attraverso le reti (ad es., VPN, HTTPS, TLS, etc.) e per gestire chiavi crittografiche.</i></p>	<p>tecniche di cifratura in quanto proprie degli strumenti informatici e delle piattaforme utilizzate dalla scuola. Anche la posta è protetta da un protocollo TLS.</p>	
<p><b>Pseudonimizzazione</b></p> <p><i>Descrizione: Misura tecnica volta a rendere anonimi e non riconducibili alla persona i dati personali trattati attraverso sistemi informatici, ad esempio attraverso l'uso di identificativi numerici in sostituzione del nome e cognome della persona.</i></p>	<p>Non viene adottata questa misura dalla scuola. Nel caso di pubblicazione degli emolumenti assegnati al personale il nome e cognome del dipendente viene sostituito da un codice numerico.</p>	<p>Non applicabile al cartaceo</p>
<p><b>Controllo degli accessi logici ed autenticazione</b></p> <p><i>Descrizione: Misure volte ad attuare e implementare la politica di controllo degli accessi logici ai dati personali trattati attraverso sistemi informatici (ad es., politiche di accesso ad applicativi o a cartelle di rete condivise), secondo ruoli e responsabilità definite e profili personali attribuiti agli utenti. Tale politica si basa sul principio della minima conoscenza: ogni utente ha accesso ai soli dati personali strettamente necessari per lo svolgimento dei propri compiti.</i></p>	<p>Gli accessi sono controllati attraverso l'impostazione di accessi limitati ai programmi che utilizza la segreteria. Il personale di segreteria in base al ruolo e al compito che svolge riceve le password e gli identificativi per l'accesso agli applicativi e ai programmi per la gestione amministrativa della scuola. Inoltre anche l'accesso alla rete e al cloud è protetto e per accedere ai pc della segreteria è necessario conoscere specifica password a disposizione del solo</p>	<p>Difficilmente applicabile per i documenti cartacei</p>

	<p>utente. Tra l'altro le password devono essere aggiornate periodicamente. Il personale deve custodire le password con cura e non comunicarle a terzi.</p> <p>Anche l'accesso al server è protetto da password.</p>	
<p><b>Cancellazione sicura</b></p> <p><i>Descrizione:</i>  <i>Misura adottata allo scopo di eliminare e distruggere irreversibilmente i dati personali, ad esempio attraverso la smagnetizzazione di un supporto informatico o la distruzione di documenti cartacei, in modo che non possano essere recuperati dal supporto su cui sono archiviati.</i></p>	<p>Tutti i computer se riutilizzati vengono ripuliti. In ogni caso nei pc degli utenti della segreteria non devono essere salvati e conservati documenti contenenti dati personali. In caso di sostituzione del server la scuola provvederà anche a togliere il disco o a smagnetizzare il supporto informatico.</p>	<p>I documenti cartacei vengono distrutti ed eliminati tramite il trita documenti.</p>

- Misure generali di sicurezza fisica e logica

Misura	Office	Cartaceo
<p><b>Sicurezza dell'ambiente operativo</b></p> <p><i>Descrizione:</i>  <i>Misure adottate per gestire la configurazione di sicurezza di server e database che costituiscono la spina dorsale del sistema di elaborazione dei dati personali, applicando politiche</i></p>	<p>Ogni pc è dotato di nome utente e password personale (non tutti posso accedere ai pc); ed anche l'accesso alle risorse di rete e al cloud è controllato e</p>	<p>Non applicabile</p>

<p><i>specifiche in funzione della rilevanza dei dati personali trattati dall'applicazione ospitata. Tali misure si applicano anche alla protezione delle applicazioni, in particolare di quelle Web.</i></p>	<p>consentito solo al personale di segreteria. Le password vengono aggiornate periodicamente. Viene consigliato al personale di scegliere password complesse e ne deve avere cura non diffondendole. Per accedere al server è necessaria una specifica password. Inoltre il server è posto in un luogo sicuro e presidiato, all'interno di un armadio rack. Una volta all'anno la ditta che fornisce consulenza informatica alla scuola controlla che il server sia configurato in modo sicuro.</p>	
<p><b>Sicurezza della rete e delle comunicazioni</b></p> <p><i>Descrizione: Misure adottate per proteggere i dati personali durante il transito attraverso la rete, sia per le connessioni esterne (Internet), sia per l'interconnessione con i sistemi del MIUR. A seconda della tipologia di canale sul quale il trattamento è effettuato, gli strumenti di protezione adottati comprendono: firewall, sonde di rilevamento intrusione e altri dispositivi attivi o passivi di sicurezza della rete, protocolli di cifratura, politiche di controllo dei cookies, etc.</i></p>	<p>I dati vengono scambiati con il sito del Ministero dell'Istruzione che è in https. Anche il sito della scuola è in https. I pc della scuola che utilizza la segreteria per lo scambio di dati sono protetti tramite antivirus e antimalware. Inoltre la scuola ha impostato un firewall di rete. La</p>	<p>Non applicabile</p>

	<p>connessione alla rete internet della segreteria è separata rispetto a quella della didattica (sono due linee distinte).</p> <p>La scuola ha inoltre adottato uno specifico regolamento che autorizza l'uso della rete internet della didattica solo per i dispositivi di proprietà della scuola e dei docenti. È fatto divieto agli insegnanti di diffondere la WPA di accesso alla rete internet.</p>	
<p><b>Tracciatura e monitoraggio</b></p> <p><i>Descrizione:</i>  <i>Misure per la registrazione delle attività eseguite su sistemi informatici dagli utenti e dagli amministratori di sistema su dati personali e sistemi di sicurezza, al fine di consentire il tracciamento delle operazioni svolte. Il monitoraggio delle registrazioni prodotte (c.d. "file di log"), inoltre, consente l'identificazione di potenziali tentativi interni o esterni di violazione del sistema e la rilevazione tempestiva di incidenti relativi a dati personali (ad es., eventi di diffusione, modifica o distruzione non autorizzate di dati personali), fornendo al tempo stesso gli elementi di prova nel contesto delle indagini</i></p>	<p>Allo stato attuale il sistema operativo non monitora i file di log.</p> <p>Inoltre i sistemi operativi gestiti dai fornitori esterni di gestionali scolastici su piattaforme cloud registrano gli event-log. Gli accessi degli utenti sono perciò monitorati e ciò è garantito dall'univocità delle credenziali assegnate ad ogni utente utilizzatore.</p>	Non applicabile
<p><b>Gestione sicura del cambiamento</b></p> <p><i>Descrizione:</i>  <i>Esistenza ed attuazione di un processo</i></p>	<p>Per politiche interne e regolamenti non è possibile che il personale modifichi</p>	Non applicabile

<p><i>operativo di gestione sicura del cambiamento al fine di controllare, attraverso verifiche e approvazioni, le modifiche eseguite nel sistema IT utilizzato per il trattamento dei dati personali. Ogni modifica deve essere registrata e la data/orario dell'ultima modifica deve essere conservata</i></p>	<p>il sistema e i programmi installati sul personal computer in uso. Anche il download di materiale da internet è sottoposto a restrizioni da specifiche politiche e istruzioni interne.</p>	
<p><b>Gestione sicura dell'hardware, delle risorse e dei dispositivi</b></p> <p><i>Descrizione: Misure adottate per gestire l'inventario e la configurazione di sicurezza dell'hardware, delle risorse di rete e dei dispositivi (server, periferiche, dispositivi di comunicazione, etc.) utilizzati per il trattamento dei dati personali.</i></p>	<p>Tutti i computers della scuola sono inventariati. I computer consegnati in comodato d'uso alle famiglie oltre che inventariati sono stati anche tutti tracciati. Inoltre tutti i pc consegnati in comodato per specifica politica interna prima della consegna vengono configurati, controllati hardware e ripuliti. I pc della segreteria vengono controllati su richiesta del personale.</p>	Non applicabile
<p><b>Gestione sicura delle postazioni di lavoro</b></p> <p><i>Descrizione: Misure adottate per gestire la configurazione di sicurezza delle postazioni di lavoro degli utenti fisse e portatili (ad es., impostazioni del sistema operativo, applicazioni, software di office automation, etc.). Tali politiche impediscono agli utenti di eseguire azioni che potrebbero compromettere la sicurezza del sistema IT (ad es., la disattivazione di programmi antivirus o l'installazione e l'esecuzione di</i></p>	<p>I computer della segreteria e il server sono oggetto di verifica annuale da parte della ditta informatica che fornisce assistenza alla scuola adotta le precauzioni di sicurezza necessarie. Per qualsiasi altra problematica interviene</p>	Non applicabile

<p><i>software non autorizzato, accesso a siti potenzialmente pericolosi).</i></p>	<p>immediatamente il Team digitale della scuola (composto dal ds, un docente e un applicativo di segreteria). Su tutti i pc della segreteria è installato e/o aggiornato l'antivirus. Sono presenti inoltre sui pc filtri anti spam e il personale amministrativo è stato anche formato sulle verifiche da porre in essere prima dell'apertura della posta istituzionale.</p>	
<p><b>Backup e Continuità operativa</b></p> <p><i>Descrizione: Esistenza ed attuazione di politiche che stabiliscono le modalità di salvataggio dei dati personali, allo scopo di assicurarne la disponibilità e l'integrità nel tempo, e di ripristino dell'operatività a seguito di un evento avverso, ossia le procedure operative e le misure tecniche da seguire per ripristinare la disponibilità e l'accesso ai servizi essenziali in caso di incidente che ne pregiudichi l'operatività.</i></p>	<p>I dati della scuola in parte vengono salvati su piattaforme esterne e sistemi dei fornitori esterni in cloud. Inoltre il personale deve lavorare salvando i documenti prodotti nelle cartelle di rete condivise sul server e su queste viene fatto il backup per permettere di ripristinare la disponibilità e l'accesso ai dati in caso di incidenti che potrebbero pregiudicarne la disponibilità.</p>	Non applicabile
<p><b>Manutenzione delle apparecchiature</b></p>	<p>Vengono svolti, su</p>	Non applicabile

<p><i>Descrizione:</i> Esistenza e attuazione di politiche per la manutenzione periodica delle apparecchiature di continuità elettrica, dei sistemi antincendio e di ogni altra tipologia di sistema a supporto dell'operatività dei sistemi informativi</p>	<p>segnalazione e richiesta del personale, controlli sulle apparecchiature come i gruppi di continuità del server e sui rilevatori di fumi. Periodicamente vengono controllati gli estintori nei locali scolastici.</p>	
<p><b>Protezione dalle fonti di rischio ambientali</b></p> <p><i>Descrizione:</i> Misure adottate per ridurre o contenere i rischi connessi a minacce ambientali (fenomeni climatici, incendi, allagamenti) che potrebbero influire sull'operatività dei sistemi informativi, sulla continuità dei servizi erogati e sulla sicurezza dei dati personali trattati. Esempi sono: gruppi di continuità, sistemi antincendio, armadi ignifughi, etc.</p>	<p>Le minacce ambientali sono oggetto di valutazione e di protezione da parte del RSPP, inoltre la scuola utilizza gruppi di continuità per il server nonché sono presenti nei locali scolastici degli estintori e rilevatori di fumi.</p>	<p>Le minacce ambientali sono oggetto di valutazione e di protezione da parte del RSPP, inoltre sono a disposizione in caso di incendio degli estintori e rilevatori di fumi.</p>

- **Misure organizzative e processi di governo**

Misura	Office	Cartaceo
<p><b>Modello Organizzativo e di Gestione</b></p> <p><i>Descrizione:</i> Il modello organizzativo e di gestione della privacy costituisce il fondamento per la sicurezza dei dati personali trattati dall'organizzazione, definendo i processi volti a controllare i rischi che i trattamenti dell'organizzazione pongono sui diritti e le</p>	<p>E' stato definito un organigramma privacy. Tutto il personale è stato designato autorizzato al trattamento dei dati personali e ha ricevuto le istruzioni</p>	<p>E' stato definito un organigramma privacy. Tutto il personale è stato designato autorizzato al trattamento dei dati personali e ha ricevuto le istruzioni</p>

<p><i>libertà delle persone interessate e individuando ruoli e responsabilità di chi ha accesso ai dati personali, in base al principio del minimo privilegio. Un ruolo di particolare importanza è svolto dal Responsabile della Protezione dei Dati (RPD), che monitora la conformità al regolamento e collabora con il Titolare nell'adeguare le misure di protezione dei dati personali trattati.</i></p>	<p>su come trattare i dati. La scuola ha poi provveduto a nominare il Dott. Federico Croso quale proprio responsabile della protezione dei dati. Il titolare del trattamento ha, inoltre, redatto il registro delle attività, ai sensi dell'art. 30 del GDPR.</p>	<p>su come trattare i dati. La scuola ha poi provveduto a nominare il Dott. Federico Croso quale proprio responsabile della protezione dei dati. Il titolare del trattamento ha, inoltre, redatto il registro delle attività, ai sensi dell'art. 30 del GDPR.</p>
<p><b>Politiche e procedure per la protezione dei dati personali</b></p> <p><i>Descrizione: La politica per la protezione dei dati personali dimostra l'impegno generale alla protezione dei dati personali e definisce i principi di base per la loro sicurezza e protezione. Il documento formalizza gli obiettivi e le regole da applicare nel campo della protezione dei dati e costituisce la base per l'attuazione delle misure tecniche e organizzative specifiche richieste dall'art. 32 del RGPD. Le specifiche misure tecniche e organizzative attuate sono descritte in procedure operative di dettaglio che indirizzano temi specifici (ad esempio controllo degli accessi, gestione dei dispositivi, gestione delle risorse, ecc.).</i></p>	<p>Il personale è stato formato in merito agli adempimenti da porre in essere per proteggere i dati dei propri interessati. E' stata adottata una politica sulla protezione dei dati. La scuola ha redatto per ciascun trattamento le specifiche informative privacy. Infine, ogni anno vengono analizzate le misure tecniche e organizzative implementate dalla Scuola.</p>	<p>Il personale è stato formato in merito agli adempimenti da porre in essere per proteggere i dati dei propri interessati. E' stata adottata una politica sulla protezione dei dati. La scuola ha redatto per ciascun trattamento le specifiche informative privacy. Infine, ogni anno vengono analizzate le misure tecniche e organizzative implementate dalla Scuola.</p>
<p><b>Gestione dei Responsabili del trattamento e delle terze parti</b></p> <p><i>Descrizione: I rapporti con fornitori esterni di servizi che hanno accesso a o trattano dati personali per conto del Titolare devono essere formalizzati tramite un contratto o altro atto legale stabilito e siglato tra le parti, in cui è disciplinato il trattamento da parte del responsabile e specificate le misure tecniche e organizzative adottate nel rispetto dei</i></p>	<p>I responsabili del trattamento sono stati identificati e nominati.</p>	<p>I responsabili del trattamento sono stati identificati e nominati.</p>

<i>requisiti del RGPD e a garanzia della tutela dei diritti dell'interessato.</i>		
<p><b>Sicurezza del ciclo di vita delle applicazioni e nei progetti</b></p> <p><i>Descrizione:</i>  Misure specifiche predisposte per garantire che si considerino i requisiti di protezione dei dati personali e l'applicazione delle più severe impostazioni sulla privacy sin dalle prime fasi del processo di sviluppo di un sistema informativo e durante il ciclo di vita delle applicazioni, nel rispetto dei principi di "Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita" introdotti dall'art. 25 del RGPD.</p>	Tutti i sistemi dal registro elettronico alle piattaforme utilizzate sono implementate secondo le raccomandazioni del GDPR e dell'AgID. I fornitori dei servizi devono infatti garantire alla scuola l'adesione alle attuali norme in materia di trattamento dei dati	Non applicabile
<p><b>Gestione degli Incidenti di sicurezza e delle Violazioni dei dati personali</b></p> <p><i>Descrizione:</i>  Nel caso si verificano incidenti di sicurezza che comportano la "distruzione, perdita, modifica, divulgazione non autorizzata o accesso ai dati personali trasmessi, conservati o comunque trattati" (cfr. art. 4.12 del RGPD), sono attivate procedure per la gestione di tali eventi e la notifica all'autorità di controllo e alle persone interessate.</p>	Adozione di una procedura per gestione data breach e predisposizione di registro delle violazioni.	Adozione di una procedura per gestione data breach e predisposizione di registro delle violazioni.
<p><b>Gestione e formazione del personale</b></p> <p><i>Descrizione:</i>  Misure specifiche predisposte per garantire che il personale coinvolto nel trattamento dei dati personali sia adeguatamente informato in merito agli obblighi di riservatezza, specialmente per il personale chiave coinvolto nel trattamento dei dati personali ad alto rischio, e sensibilizzato sulle procedure di sicurezza e protezione dei dati (ad esempio uso di password e accesso a specifici sistemi di elaborazione e trasmissione dati).</p>	Nomine persone autorizzate e formazione.	Nomine persone autorizzate e formazione.
<b>Controllo degli accessi fisici</b>	I collaboratori scolastici sono	I collaboratori scolastici sono

<p><i>Descrizione:</i>  <i>Misure volte ad assicurare la sicurezza fisica e il controllo degli accessi agli edifici e alle zone in cui sono ospitate le risorse a supporto del trattamento (documenti cartacei e strumenti informatici), ad esempio attraverso un servizio di portineria, l'uso di tornelli con autenticazione tramite badge di riconoscimento e porte chiuse a chiave.</i></p>	<p>incaricati di monitorare le entrate e le uscite.</p>	<p>incaricati di monitorare le entrate e le uscite.</p>
<p><b>Sicurezza dei documenti cartacei</b></p> <p><i>Descrizione:</i>  <i>Politiche e processi di gestione dell'archivio per assicurare che i documenti cartacei contenenti dati personali utilizzati durante il trattamento siano prodotti, archiviati, consultati, trasmessi e distrutti nel rispetto dei diritti dell'interessato.</i></p>	<p>Non applicabile</p>	<p>I documenti cartacei, per prassi, vengono conservati e archiviati all'interno dell'ufficio della segreteria e della dirigente in armadi chiusi a chiave; l'ingresso ai locali è monitorato dal personale presente. In caso di assenza del personale gli uffici vengono chiusi a chiave. I documenti altamente sensibili e i fascicoli riservati sono custoditi in cassaforte. I documenti non più in uso vengono archiviati in un apposito locale, chiuso a chiave, il cui accesso è consentito al solo personale autorizzato.</p>