GDPR SCUOLA

LO STAFF TECNICO DEL DIRIGENTE

MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE ADOTTATE, AI SENSI DELL'ART. 32 DEL GDPR, DALL'ISTITUTO COMPRENSIVO "GALILEO GALILEI" GRAVELLONA TOCE

(**Verbale Audit 22.04.2021**)

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 "Galileo Galilei" di Gravellona Toce:

- # Misure specifiche per la protezione dei dati

Misura	Office	Cartaceo
Minimizzazione della quantità di dati personali *Descrizione:* *Misure volte a gestire solo dati personali adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.*	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.	Vengono trattati i dati degli utenti in moda da rispettare il principio di minimizzazione.
Partizionamento dei dati *Descrizione:* *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.*	I documenti digitali vengono archiviati in cloud tramite il programma della segreteria digitale. Alcuni dati vengono partizionati in cartelle e condivisi sul server della segreteria. Inoltre i documenti vengono altresì protocollati con protocollo riservato o ordinario.	I dati vengono suddivisi in faldoni o archivi separati con titolario di classificazione.
Cifratura	Il sito della scuola è	No

Descrizione: *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.*	in https ed inoltre vengono adottate tecniche di cifratura in quanto proprie degli strumenti informatici e delle piattaforme utilizzate dalla scuola. Anche la posta è protetta da un protocollo TLS. Infine per prassi interna i documenti che la scuola invia alla Ragioneria Territoriale dello Stato di Novara sono cifrati.	
Pseudonimizzazione *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.*	Non viene adottata questa misura dalla scuola.	Non applicabile al cartaceo
Controllo degli accessi logici ed autenticazione *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.*	Gli accesi 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 è	Difficilmente applicabile per i documenti cartacei

	protetto e per accedere ai pc della segreteria è necessario conoscere specifica password a disposizione del solo utente. Tra l'altro le password devono essere aggiornate periodicamente. Il personale deve custodire le password con cura e non comunicarle a terzi. Anche l'accesso al server è protetto da password.	
Cancellazione sicura *Descrizione:* *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 computer non più in uso se riutilizzati o consegnati in comodato alle famiglie vengono formattati e ripuliti. In caso di dismissione dei pc i medesimi vengono smaltiti dalla ditta incaricata dalla scuola.	I documenti cartacei vengono distrutti ed eliminati tramite il trita documenti.

- Misure generali di sicurezza fisica e logica

Misura	Office	Cartaceo
Sicurezza dell'ambiente operativo *Descrizione:* *Misure adottate per gestire la configurazione di sicurezza di server e database che costituiscono la spina dorsale del sistema di elaborazione dei*	Ogni pc è dotato di nome utente e password personale (non tutti posso accedere ai pc); ed anche l'accesso alle risorse di rete è	Non applicabile

dati personali, applicando politiche 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.	controllato e 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 a disposizione dell'amministratore di sistema. Inoltre il server è posto in un luogo sicuro, dedicato e protetto.	
Sicurezza della rete e delle comunicazioni *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 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 connessione alla rete internet della segreteria è separata rispetto a quella della didattica.	Non applicabile

Tracciatura e monitoraggio *Descrizione:* *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*	Ogni postazione della segreteria ha un log utente numerato e ogni operazione fatta all'interno della rete è tracciata. Anche gli ingressi dell'amministratore di sistema sono tracciati. 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.	Non applicabile
Gestione sicura del cambiamento *Descrizione:* *Esistenza ed attuazione di un processo 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*	La scuola ha previsto che il personale autonomamente non può modificare il sistema e i programmi installati sul personal computer in uso; per ogni modifica è necessario l'intervento e la password dell'amministratore di rete.	Non applicabile
Gestione sicura dell'hardware, delle risorse e dei dispositivi *Descrizione:*	Tutti i computers della scuola sono inventariati. I pc vengono controllati su richiesta del	Non applicabile

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.	personale. Periodicamente l'amministratore di sistema verifica che il server ed i pc siano configurati in modo sicuro.	
Gestione sicura delle postazioni di lavoro *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 software non autorizzato, accesso a siti potenzialmente pericolosi).*	I computer sono oggetto di periodica verifica da parte dell'amministratore di sistema che adotta le precauzioni di sicurezza necessarie. Inoltre tutti gli interventi sui pc che potrebbero compromettere la sicurezza del sistema IT devono essere autorizzati. Su tutti i pc della segreteria è istallato e/o aggiornato l'antivirus. Tutti i pc sono poi protetti tramite il firewall di rete che blocca eventuali minacce e l'accesso a siti potenzialmente pericolosi. Le macchine del personale di segreteria inoltre bloccano lo schermo in caso di non uso del pc e di allontanamento.	Non applicabile
Backup e Continuità operativa *Descrizione:* *Esistenza ed attuazione di politiche che stabiliscono le modalità di salvataggio dei dati personali, allo scopo di assicurarne la*	Il personale deve lavorare salvando i documenti prodotti nelle cartelle di rete sul server e viene fatto il backup in	Non applicabile

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.	cloud per permettere di ripristinare la disponibilità e l'accesso ai dati in caso di incidenti che potrebbero pregiudicarne la disponibilità. I documenti digitali inoltre vengono archiviati anche in cloud tramite il programma Argo Gecodoc.	
Manutenzione delle apparecchiature *Descrizione:* *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*	Vengono svolti, su segnalazione e richiesta del personale, controlli sulle apparecchiature come i gruppi di continuità del server. Periodicamente vengono controllati gli estintori nei locali scolastici CO2.	Non applicabile
Protezione dalle fonti di rischio ambientali *Descrizione:* *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.*	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 CO2.	Le minacce ambientali sono oggetto di valutazione e di protezione da parte del RSPP, inoltre sono a disposizione in caso di incendio degli estintori CO2.

- Misure organizzative e processi di governo

Misura	Office	Cartaceo
Modello Organizzativo e di Gestione *Descrizione:* *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 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.*	E' stato definito un organigramma privacy. Tutto il personale è stato designato autorizzato al trattamento dei dati personali e ha ricevuto le istruzioni su come trattare i dati; la scuola ha inoltre provveduto a nominare il Dott. Federico Croso quale proprio responsabile della protezione dei dati.	E' stato definito un organigramma privacy. Tutto il personale è stato designato autorizzato al trattamento dei dati personali e ha ricevuto le istruzioni su come trattare i dati; la scuola ha inoltre provveduto a nominare il Dott. Federico Croso quale proprio responsabile della protezione dei dati.
Politiche e procedure per la protezione dei dati personali *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.).*	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 e redatto il registro delle attività di trattamento in cui vengono definiti i trattamenti posti in essere dalla scuola. Sono state adottate inoltre delle check list relative agli adempimenti in materia di privacy e di sicurezza per i dati.	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 e redatto il registro delle attività di trattamento in cui vengono definiti i trattamenti posti in essere dalla scuola. Sono state adottate inoltre delle check list relative agli adempimenti in materia di privacy e di sicurezza per i dati.
Gestione dei Responsabili del trattamento e delle terze parti	I responsabili del trattamento sono	I responsabili del trattamento sono

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 requisiti del RGPD e a garanzia della tutela dei diritti dell'interessato.*	stati identificati e nominati.	stati identificati e nominati.
Sicurezza del ciclo di vita delle applicazioni e nei progetti *Descrizione:* *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.*	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
Gestione degli Incidenti di sicurezza e delle Violazioni dei dati personali *Descrizione:* *Nel caso si verifichino 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.*	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.
Gestione e formazione del personale *Descrizione:* *Misure specifiche predisposte per garantire che il personale coinvolto nel trattamento dei dati personali sia adeguatamente informato in merito agli obblighi di riservatezza,*	Nomine persone autorizzate e formazione.	Nomine persone autorizzate e formazione.

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).		
Controllo degli accessi fisici *Descrizione:* *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 collaboratori scolastici sono incaricati di monitorare le entrate e le uscite. Tutti gli ingressi vengono annotati in un apposito registro dei visitatori esterni. L'accesso alla segreteria è vietato e vi è un apposito sportello esterno per eventuali richieste.	I collaboratori scolastici sono incaricati di monitorare le entrate e le uscite. Tutti gli ingressi vengono annotati in un apposito registro dei visitatori esterni. L'accesso alla segreteria è vietato e vi è un apposito sportello esterno per eventuali richieste.
Sicurezza dei documenti cartacei *Descrizione:* *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.*	Non applicabile	I documenti cartacei, per prassi, vengono conservati e archiviati all'interno dell'ufficio della segreteria in armadi; 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 implementato a norma di legge con

		porte tagliafuoco. L'archivio è chiuso a chiave e per accedervi è necessario essere autorizzati.

IL DIRIGENTE SCOLASTICO
Dott. Gino CARISSIMI
Firmato digitalmente ai sensi del D.lgs n.82/2005 s.m.i e norme collegate