TITOLARE DEL TRATTAMENTO
Istituto Comprensivo "Monda Volpi" di Cisterna di Latina

RESPONSABILE DELLA PROTEZIONE DEI DATI
OXFirm di Bove Antonio via Laurenza 49, 81027 San Felice a Cancello(CE) Tel /Fax: 0823.753477 - E-MAIL: privacy@oxfirm.it nella persona di Ing. Antonio Bove, tel.: 3397775992

INFORMAZIONI GENERALI	
Numero di plessi:	6
Numero di plessi coperti da rete:	6
Numero di postazioni amministrative (incluso DS e DSGA):	9
Numero approssimativo di device per plesso:	40
Animatore digitale:	Prof. Virginia Vuerich
Collaboratori del DS	Prof.ssa Fagiolo Flora, Prof.ssa Marcelli Rita, incaricati formalmente

Responsabile sito web interno:	Prof. Virginia Vuerich, Prof. Tretola Ernesto (esterno), incaricati formalmente
Responsabile pubblicazione:	Prof. Virginia Vuerich, incaricato formalmente
Resp. piattaforma DaD	Prof. Virginia Vuerich, incaricato formalmente
Resp. rilascio password piattaforma DaD	Prof. Virginia Vuerich, incaricato formalmente
Referente Covid	Dir. Nunzia Malizia, Fagiolo Flora, incaricato formalmente
Resp. raccolta autodic. e mis. temp.	Tutti i collaboratori di ingresso, non applicabile
Amministratore di sistema interno:	incaricato formalmente
Responsabile di plesso:	Marcelli Rita (plesso A. Volpi - centrale), Tartara Emanuela, Fanesi Vittoria (Dante Monti - primaria), Moi Arcangela (Infanzia - Monti Lepini), Patrizia Pascale (Infanzia - Rosa Rosaria Tomei), Sogliano Antonella (Infanzia Borgo Flora), Danesin Nadia (Primaria - Borgo Flora), incaricato formalmente
Gestionale Segreteria:	Axios Italia Service s.r.l. (segreteria digitale),
Registro Elettronico:	ClasseViva di Spaggiari (con totem)

RESPONSABILI ESTERNI DEL TRATTAMENTO	
Fornitore assistenza tecnica:	LG Infotech (Mauro, si, incarico formalizzato)

Fornitore noleggio fotocopiatori:	Digital Copy srl di Latina, si, incarico formalizzato
RSPP:	Ing. Peretti Pier Giuseppe, si, incarico formalizzato
Medico competente:	Dott.ssa Miola Alessandra, si, incarico formalizzato
Psicologo:	n.a.
Altri responsabili esterni del trattamento:	

LE MISURE DI SICUREZZA

L'art. 32 del Regolamento Europeo 679/2016 fissa alcuni principi fondamentali. In particolare le misure di sicurezza devono essere approntate "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".

Le misure di sicurezza, quindi, devono essere adeguate e ragionevolmente soddisfacenti alla luce delle conoscenze e delle prassi con l'obiettivo della tutela dei dati.

Le misure di sicurezza possono essere di natura tecnica e organizzative, e comprendono, tra le altre la **pseudonimizzazione**, la **cifratura** dei dati personali e **requisiti di sicurezza** intesi come:

- la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- la capacità di **ripristinare** tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- presenza di procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

A seguito della verifica effettuata dal Responsabile della Protezione dei dati in data 04/06/2021 è stato rilevato lo stato delle Misure di Sicurezza.

MISURE DI SICUREZZA TECNICHE FISICHE

Per approntare delle misure di sicurezza "adeguate" è necessario valutare una serie di fattori quali:

- le modalità di accesso ai locali (prevedendo quali aree ed in quali orari potrà essere consentito l'accesso al pubblico o al personale non autorizzato);

- la qualità delle protezioni esterne come porte e serrature, la presenza di allarmi, illuminazione di sicurezza o CCTV (telecamere);

- la corretta gestione e smaltimento dei rifiuti cartacei o elettronici;

- l'impostazione delle apparecchiature informatiche e le politiche del loro utilizzo, incluse quelle di proprietà dell'utente quando queste possono connettersi alla rete dell'Amministrazione. (Tra le indicazioni di AgID vie è quella della tenuta di un registro con l'indicazione delle risorse informatiche utilizzate per trattare dati, la loro ubicazione fisica e i permessi di accesso alle stesse, ecc.).

- L'ingresso all'edificio è presidiato da collaboratori scolastici e avviene previo utilizzo di campanello.
- L'accesso agli uffici amministrativi è presidiato da collaboratori scolastici.
- Gli uffici amministrativi sono tutti collocati in una sezione dedicata dell'edificio.
- Negli uffici amministrativi sono presenti: grate, porte blindate, chiusura a chiave, armadi con serratura, casseforti/armadi blindati.
- Presenza di un front office: è presente un front office per gli alunni e famiglie ed uno per il personale

Il front office è utile per accogliere genitori, studenti ed insegnanti in modo da limitare al massimo l'accesso di personale estraneo all'interno degli uffici amministrativi e di tutelare la privacy e la sicurezza dei dati.

- La pulizia degli uffici amministrativi viene effettuata da collaboratori scolastici e dovrebbe essere inibito l'accesso a tutti i locali che contengono dati particolari.

- Il sistema di allarme: è presente in tutto l'edificio in ogni plesso; è presente in tutto l'edificio solo nella sede centrale.
- Il sistema di videosorveglianza: non è presente. La gestione della videosorveglianza è non applicabile. La conservazione dei dati (luogo) è non applicabile.
    - Accesso a NAS/NVR/DVR con password: non è presente.
    - Dispositivo di conservazione in armadio protetto: non è presente.
    - Sistema di conservazione criptato: non è presente.
    - Monitor ripresa in diretta: non è presente.
- Sistema antincendio: è presente tutto l'edificio.
- Gruppi di continuità: presente solo sul/sui server, sul NAS.
- È presente un sistema di distruzione dei documenti cartacei. È importante garantire la sicurezza dei dati attraverso la distruzione di documenti o fotocopie non più utilizzati. È consigliabile custodire i documenti cartacei e i supporti informatici removibili in scaffali chiusi a chiave e al termine dell'orario di lavoro riporre tutti i documenti presenti sulla scrivania in cassetti chiusi a chiave, soprattutto quando la pulizia degli uffici è affidata a ditte esterne.

MISURE DI SICUREZZA TECNICHE LOGICHE

Misure di sicurezza suggerite:

Poiché il processo di gestione dei dati passa sempre, in un determinato momento, attraverso attrezzature informatiche, uno dei principali fattori da considerare è la messa in sicurezza delle attrezzature stesse.

La sicurezza nell'informatica equivale ad attuare tutte le misure e tutte le tecniche necessarie per proteggere l'hardware, il software e i dati dagli accessi non autorizzati (illegali o accidentali), per garantirne la riservatezza, nonché eventuali usi illeciti, dalla divulgazione, modifica e distruzione.

La trasposizione dell'attuale normativa europea in materia di implementazione delle misure di sicurezza logiche pone ai Titolari e ai Responsabili del trattamento dei dati numerosi adempimenti, molti dei quali di non semplice e pronta attuazione, benché non richiedano

l'impiego di risorse economiche. In particolare, l'adozione di "misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio" suggerisce la configurazione differenziata delle varie attrezzature in rapporto al loro impiego concreto nella gestione dei dati personali.

Nel corso della verifica è stato rilevato lo stato delle seguenti misure di sicurezza logiche:

Misure digitali

- Dominio Windows: è presente.
- Sistema di back-up in rete locale: è presente.
- Sistema di back-up in cloud: è presente.
- Immagine fisica delle postazioni di segreteria: non applicabile.
- Accesso a cartelle condivise (con password) su Server/NAS: è presente.
- Firewall: è presente.
- Gestione di presenze elettronica: è presente.
- Gestione di presenze cartacea: non è presente.
- Separazione fisica o logica delle reti LAN per la didattica e la segreteria: è presente.
- Sistema di stampanti di rete: è presente.

Configurazione PC

Per la **segreteria** sono presenti le seguenti misure di sicurezza per il PC:

doppio account (amministratore/utente), aggiornamenti automatici sistemi operativi, aggiornamenti antivirus automatizzati, accesso tramite password, sospensione automatica delle sessioni di lavoro (screensaver con password).

Per la **didattica** sono presenti le seguenti misure di sicurezza per il PC:

aggiornamenti automatici sistemi operativi, aggiornamenti antivirus automatizzati.

È consigliabile che le misure di sicurezza per i PC includano sempre: creazione di doppio account (amministratore e utente limitato) protetti da password, impostazione degli aggiornamenti del sistema operativo, dell'antivirus, e di tutte le applicazioni automatica,

sospensione automatica delle sessioni di lavoro (screensaver con password) con un tempo di attivazione non superiore ai 5 minuti e con riavvio protetto da password.
Si raccomanda di creare sempre delle password di accesso di complessità adeguata (contenenti almeno 8 caratteri, maiuscole, minuscole, lettere e numeri ed un carattere speciale) le quali dovranno essere cambiate periodicamente; le password inoltre non devono essere annotate su foglietti custoditi nei pressi della postazione o sotto la tastiera.
Si consiglia di custodire le password create e/o modificate in armadi chiusi a chiave le quali dovranno essere consegnate in busta chiusa all'amministratore di sistema. Ogni cambio di password dovrà essere appositamente annotato nel relativo registro.
Si consiglia di creare accessi logici e di autenticazione ad applicativi o a cartelle condivise secondo ruoli e responsabilità definiti e profili personali attribuiti agli utenti al fine di migliorare la sicurezza e la gestione dei dati archiviati.
Si suggerisce inoltre di separare i dati particolari e/o giudiziari da quelli non particolari e/o giudiziari in partizioni diverse - nonché applicare controlli di sicurezza diversi ai dati particolari.
Si consiglia di registrare ogni intervento e/o modifica eseguita nel sistema informatico da parte dell'amministratore. Ogni modifica deve essere registrata e la data/orario dell'ultima modifica deve essere conservata.

Si consiglia di effettuare una verifica periodica delle attrezzature informatiche, nonché di eseguire una verifica dell'operato degli addetti alla manutenzione.

In ogni caso sarebbe opportuno conformarsi alle indicazioni di AgID in materia di misure minime di sicurezza per le pubbliche amministrazioni (circolare AgID 2/2017).

Navigazione internet

Per la **segreteria** sono presenti le seguenti misure di sicurezza per la navigazione internet:

autenticazione univoca alla rete LAN (account e pw personali), filtraggio della navigazione, aggiornamento black list internazionali.

Per la **didattica** sono presenti le seguenti misure di sicurezza per la navigazione internet:

autenticazione univoca alla rete Wi-Fi (account e pwd personali), filtraggio della navigazione, aggiornamento black list internazionali.

È consigliabile che le misure di sicurezza per la navigazione internet includano: autenticazione univoca alla rete Wi-Fi (account e pwd personali), autenticazione univoca alla rete LAN (account

e pwd personali), filtraggio della navigazione, aggiornamento black list internazionali, blocco traffico da geolocalizzazione. E'consigliabile, inoltre, effettuare gli aggiornamenti delle black list il più frequentemente possibile e, comunque, ad intervalli non superiori ad una settimana.

Gestione dati

Si consiglia di adottare delle soluzioni di backup che consentano di proteggere il sistema operativo, le applicazioni software e la parte dati da eventuali perdite accidentali attraverso software in grado di eseguire le copie di salvataggio dei dati presenti su tutte le postazioni verso una cartella criptata sul server in modo automatico e con cadenza giornaliera.

Si consiglia di effettuare le copie di backup dei dati salvati sul server su dispositivi esterni (hd esterni o meglio NAS collegati in rete o meglio ancora direttamente nel Cloud), in modo automatico e con cadenza giornaliera. Tali dispositivi dovranno essere infine custoditi in appositi armadi chiusi a chiave.

Nel caso in cui il salvataggio dei dati nel Cloud venga eseguito dalla Scuola mediante l'utilizzo di software e Cloud gestiti direttamente dal fornitore, quest'ultimo dovrà essere designato Responsabile esterno del trattamento dei dati.

Viceversa, se la Scuola acquista il software da terzi e utilizza un proprio spazio web sarà opportuno verificare che il software adotti tutti i protocolli di sicurezza previsti dalla normativa vigente.

Assicurarsi che i software di gestione presenti all'interno del proprio edificio siano conformi al GDPR mediante richiesta al fornitore.

Si consiglia infine:

- La definizione di procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento: presente.
- La verifica periodica delle attrezzature da parte dell'amministratore di sistema: non presente.
- La verifica dell'operato degli addetti alla manutenzione: non presente.

MISURE DI SICUREZZA ORGANIZZATIVE

L'art. 5, par. 1, lett. f), impone che i dati personali debbano essere "*trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»)*". E' l'intero trattamento a dover essere sicuro, non solo i dati in quanto tali. La sicurezza, infatti, non riguarda solo l'aspetto "logico" del trattamento, ma anche l'aspetto organizzativo posto alla base dei processi di trattamento.

Tra le misure organizzative si rilevano le seguenti:

- registro del Titolare, informativa per il trattamento dei dati personali dei fornitori, informativa per il trattamento dei dati personali dei dipendenti, informativa per il trattamento dei dati personali degli alunni e delle famiglie, incarico docenti, incarico personale segreteria, stampa e protocollazione del registro, impegnativa alternanza scuola-lavoro, organigramma Privacy, gestione e formazione del personale

Ricordiamo che il **Registro del Titolare del Trattamento** rappresenta uno strumento di pianificazione e controllo della politica della sicurezza di dati e banche di dati, tesa a garantire la loro integrità, riservatezza e disponibilità. Esso è altresì uno strumento fondamentale e indispensabile per ogni valutazione e analisi del rischio. Si ricorda che tale registro, oltre ad essere datato e protocollato, andrà necessariamente aggiornato e modificato ogni volta in cui i trattamenti ivi indicati subiranno delle modifiche.

Infine si suggerisce:

- la predisposizione e pubblicazione sul sito web della scuola, nella sezione privacy, delle **informative** riguardanti il trattamento dei dati dei fornitori, dipendenti e alunni delle famiglie. Si fa presente che il Titolare del trattamento, in virtù del principio dell'accountability dovrà dare massima diffusione alle stesse utilizzando differenti canali (a titolo esemplificativo tramite pubblicazione sul sito istituzionale della scuola in un'apposita sezione PRIVACY posta in calce alla pagina e sempre visibile, nonché tramite posta elettronica, registro elettronico ecc...);
- la designazione dei **responsabili esterni del trattamento** dei dati. A tal proposito si precisa che dovranno essere nominati responsabili esterni del trattamento dei dati tutte quelle persone sia fisiche sia giuridiche, legate all'Amministrazione da un contratto avente natura non

occasionale ma continuativa e che trattano i dati personali per conto del Titolare del Trattamento (ossia della Scuola). Si pensi ad esempio al gestore del registro elettronico e contabilità, all'amministratore di sistema esterno.
Inoltre potranno essere nominati responsabili esterni del trattamento dei dati il medico del lavoro, il responsabile della sicurezza, gli esperti esterni. In assenza di tale nomina sarebbe comunque opportuno integrare i relativi contratti con clausole di riservatezza previste nel modello di responsabile esterno del trattamento.

- l'individuazione di un **amministratore di sistema** interno o esterno all'Istituzione Scolastica che avrà il compito di sovrintendere all'aggiornamento dei sistemi operativi, delle applicazioni e di tutte le attrezzature secondo le indicazioni fornite dal Titolare del trattamento;
- le designazioni del **personale incaricato/autorizzato** al trattamento dei dati personali che potranno essere sottoscritte dal personale interessato per presa visione;
- la compilazione del **diario della privacy** all'interno del quale annotare le attività eseguite per la conformità dell'Istituzione Scolastica al reg. UE 2016/679 nonché tutti gli incontri, colloqui telefonici, mail intercorse con il Responsabile della Protezione dei Dati.

San Felice a Cancello, 04/06/2021

Ing. Antonio Bove