Unione Europea

FONDI STRUTTURALI EUROPEI

PON 2014-2020

MIUR

PER LA SCUOLA - COMPETENZE E AMBIENTI PER L'APPRENDIMENTO (FSE-FESR)

ISTITUTO COMPRENSIVO LARGO VOLUMNIA

Ministero dell' Istruzione, dell'Università e della Ricerca
Ufficio Scolastico Regionale per il Lazio

Istituto Comprensivo Largo Volumnia

00181 Roma – Tel. 06 7840931 – Fax 06 7803254
e-mail rmic8gc00n@istruzione.it
C.M. RMIC8GC00N - C.F. 80246110581

PIANO SICUREZZA INFORMATICA

FINALITA' E SCOPI

A seguito della Direttiva del Presidente del Consiglio dei Ministri 1 agosto 2015 che impone a tutte le PA l'adozione nel più breve tempo possibile di standard minimi di prevenzione e reazione ad eventi cibernetici ed a seguito della circolare dell'AGID n. 2/2017 del 18/04/2017 dal titolo "Misure minime di sicurezza ICT per le pubbliche amministrazioni", secondo la quale tutte le amministrazioni pubbliche devono conseguire le misure minime di sicurezza ICT specificate in un allegato alla circolare, viene elaborato il presente documento, al fine di mettere in atto le misure di sicurezza per tutelare i dati personali oggetto di trattamento ed inoltre quelle organizzative, fisiche e logistiche, adottate nel presente anno scolastico 2017/2018 e da adottare per il trattamento dei dati personali, effettuato da tutto il personale dell'Istituto Comprensivo Statale "Largo Volumnia"di Roma, il cui rappresentante pro-tempore è il **Dirigente Scolastico, prof.ssa Maria Rosaria Merolla**, che nel seguito del documento sarà indicato come "**Titolare**". Il **Responsabile del trattamento** è il **Direttore dei Servizi Generali e Amministrativi** che nomina e coordina gli incaricati**:** assistenti amministrativi deputati al trattamento dei dati (gestione e conservazione password e copie di sicurezza di back-up dei dati)**.** Viene nominata **Responsabile esterno del trattamento dei dati** nella società **Argo Software s.r.l.** di Ragusa, limitatamente alla gestione del back up dei dati sul suo server remoto, tramite il programma Argo Save, e del servizio Argo Scuolanext che si riferisce al sistema informatizzato con cui far interagire docenti, studenti e famiglie in tempo reale, tramite la rete internet, con crittografia. I provvedimenti organizzativi disposti e le misure di sicurezza adottate, in osservanza a quanto disposto dal D. L.vo 196/2003, sono finalizzati a garantire a ciascun "interessato" (utente, dipendente, fornitore, esperto esterno, specialista esterno) la tutela della privacy, della riservatezza dei dati, della dignità personale, dell'identità personale; la tutela della riservatezza delle documentazioni custodite dalla scuola e salvaguardia dell'integrità nel tempo delle documentazioni medesime, siano esse costituite da materiale cartaceo che registrate su supporti informatici.

Nei vari punti del presente "Documento", i riferimenti alle "*Regole*", sono quelli del "Disciplinare tecnico in materia di misure minime di sicurezza", allegato B al Codice D.L. 196/2003.

PRINCIPALI DEFINIZIONI

a) **Definizioni generali in materia di Privacy previste dal D.Lgs. n.196/2003:**

"**Trattamento**", ai sensi dell'art. 4 del D. L.vo 196/2003, qualunque operazione o complesso di operazioni, effettuate anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati; in particolare, per la scuola, qualsiasi operazione (raccolta, archiviazione, utilizzo, consultazione, aggiornamento, cancellazione) che può essere effettuata utilizzando i dati personali degli studenti, dei professori o di altre persone.

"**Dato personale**", qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale; in particolare, per la scuola, qualsiasi informazione che riguardi persone fisiche (come uno studente o un professore) identificate o che possono essere comunque identificate tramite ulteriori dati, quali un numero o un codice identificativo (ad esempio il cosiddetto "codice studente").

Sono, tra gli altri, dati personali: il nome e cognome, l'indirizzo di residenza, il codice fiscale, la fotografia di una persona o la registrazione della sua voce, l'impronta digitale o i dati sanitari.

"**Dati identificativi**", i dati personali che permettono l'identificazione diretta dell'interessato;

"**Dati sensibili**", i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;

"**Dati giudiziari**", i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;

"**Dato anonimo**", il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;

"**Titolare del trattamento dei dati personali**", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

In ambito scolastico, il titolare del trattamento in genere è il Ministero dell'Istruzione, dell'Università e della Ricerca, o l'Istituto scolastico di riferimento, il cui rappresentante pro tempore è il Dirigente Scolastico.

"**Responsabile del trattamento dei dati personali**", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali; in ambito scolastico, la persona (il D.S.G.A.), la società, l'ente, l'associazione o l'organismo cui il titolare può affidare (previa apposita designazione), anche all'esterno, per la particolare esperienza o capacità, compiti di gestione e controllo del trattamento dei dati.

"**Amministratore di Sistema**", figura dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali.

"**Incaricato del trattamento dei dati personali**", la persona fisica autorizzata a compiere operazioni di trattamento, dal titolare o dal responsabile; in ambito scolastico, il dipendente (un professore, un componente della segreteria, etc.) o il collaboratore che, per conto del titolare del trattamento dei dati, elabora o utilizza materialmente i dati personali sulla base delle istruzioni ricevute dal titolare medesimo (e/o dal responsabile, se designato).

"**Interessato**", la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali; in ambito scolastico ad esempio lo studente, il professore, l'esperto esterno ecc.

"**Informativa**", contiene le informazioni che il titolare del trattamento deve fornire all'interessato per chiarire, in particolare, se quest'ultimo è obbligato o meno a rilasciare i dati, quali sono gli scopi e le modalità del trattamento, l'ambito di circolazione dei dati e in che modo si possono esercitare i diritti riconosciuti dalla legge.

"**Ricorso**", va presentato al Garante per far valere i diritti di cui all'articolo 7 del Codice della privacy solo quando la risposta del titolare (o del responsabile, se designato) all'istanza con cui si esercita uno o più dei predetti diritti non è pervenuta o viene ritenuta non soddisfacente. In alternativa al ricorso al Garante, l'interessato può rivolgersi all'Autorità giudiziaria ordinaria.

"**Comunicazione**", il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

"**Diffusione**", far conoscere dati personali a uno o più soggetti determinati (che non siano l'interessato, il responsabile o l'incaricato), in qualunque forma, anche attraverso la loro messa a disposizione o consultazione.

"**Consenso**", la libera manifestazione di volontà dell'interessato con cui questi accetta espressamente un determinato trattamento dei suoi dati personali, del quale è stato preventivamente informato da chi ha un potere decisionale sul trattamento (vedi TITOLARE). È sufficiente che il consenso sia "documentato" in forma scritta (ossia annotato, trascritto, riportato dal titolare o dal responsabile o da un incaricato del

trattamento su un registro o un atto o un verbale), a meno che il trattamento riguardi dati "sensibili"; in questo caso occorre il consenso rilasciato per iscritto dall'interessato (ad esempio con la sua sottoscrizione).
"**Blocco**", la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;
"**Banca di dati**", qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;
"**Autorizzazione**", il provvedimento adottato dal Garante con cui il titolare del trattamento in ambito privato o pubblico (ad esempio la scuola) viene autorizzato a trattare determinati dati "sensibili" o giudiziari, oppure a trasferire dati personali all'estero. In materia di dati sensibili e giudiziari, il Garante ha emanato alcune autorizzazioni generali che consentono a varie categorie di titolari di trattare dati per gli scopi specificati senza dover chiedere singolarmente un'apposita autorizzazione al Garante
"**Garante**", l'autorità di cui all'articolo 153, istituita dalla legge 31.12.1996 n. 675;

b) **Definizioni tecniche previste dal D.Lgs. n. 196/2003:**
"**comunicazione elettronica**", ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato o utente ricevente, identificato o identificabile;
"**chiamata**", la connessione istituita da un servizio telefonico accessibile al pubblico, che consente la comunicazione bidirezionale in tempo reale;
"**reti di comunicazione elettronica**", i sistemi di trasmissione, le apparecchiature di commutazione o di instradamento e altre risorse che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, incluse le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito e a commutazione di pacchetto, compresa Internet, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui sono utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato;
"**rete pubblica di comunicazioni**", una rete di comunicazioni elettroniche utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico;
"**dati relativi all'ubicazione**", ogni dato trattato in una rete di comunicazione elettronica che indica la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico;
"**posta elettronica**", messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza.

c) **Definizioni sulle misure minime di sicurezza previste dal Disciplinare tecnico allegato al D.Lgs. n. 196/2003:**

"**misure di sicurezza**", sono tutti gli accorgimenti tecnici ed organizzativi, i dispositivi elettronici o i programmi informatici utilizzati per garantire che i dati non vadano distrutti o persi anche in modo accidentale, che solo le persone autorizzate possano accedervi, che non siano effettuati trattamenti contrari alle norme di legge o diversi da quelli per cui i dati sono stati raccolti.

"**misure minime**", il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'art. 31;

"**strumenti elettronici**", gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;

"**autenticazione informatica**", l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;

"**credenziali di autenticazione**", i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica;

"**parola chiave**", componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica;

"**profilo di autorizzazione**", l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti;

"**sistema di autorizzazione**", l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

Per quanto riportato emerge che i dati personali non sono perciò solo le informazioni alfanumeriche, ma tutte quelle che si riferiscono ad un soggetto, comunque identificabile; la nozione è volutamente molto ampia e in questa debbono comprendersi anche le registrazioni informatiche degli accessi tramite "badge", le immagini ed i suoni (videosorveglianza e audioregistrazioni, che costituiscono forme di trattamento di dati personali). La legge detta una serie di regole procedurali per garantire la tutela delle persone e di altri soggetti anche da queste attività.

ELENCO DEI TRATTAMENTI DI DATI PERSONALI

Descrizione sintetica

Indicazione delle finalità perseguite e delle attività svolte dall'Istituto:

- Garanzia del servizio scolastico offerto all'utenza del Comune di Roma, della provincia di Roma
- Gestione del personale interno con contratto a tempo determinato e indeterminato
- Gestione di esperti esterni per le finalità specifiche dell'offerta formativa agli alunni
- Certificazione degli esiti scolastici e dei servizi prestati dai dipendenti
- Acquisizione di beni e servizi da fornitori

Natura dei dati trattati

Documentazioni complete riguardanti gli alunni, relative al corso di studi, alla presenza di handicap, DSA, BES, alla certificazione dello stato di salute, dell'idoneità alla pratica sportiva non agonistica, alla scelta dell'insegnamento della Religione Cattolica. Documenti prodotti dalle famiglie, riguardanti la certificazione della situazione patrimoniale (ISEE). Tutta la documentazione riguardante i docenti, il personale ATA, con elementi di individuazione di appartenenza sindacale, stato di salute o credi religiosi, anche di congiunti per i quali vengono richiesti benefici previsti da particolari norme, dallo stato di servizio, alla retribuzione, alle eventuali pratiche disciplinari. Documenti relativi agli esperti, consulenti, collaboratori esterni e ai fornitori. I dati sensibili e giudiziari sono trattati previa verifica della loro pertinenza, completezza, non eccedenza ed indispensabilità rispetto alle finalità perseguite nei singoli casi, anche con riferimento ai dati che l'interessato fornisce di propria iniziativa. In ogni caso, per l'identificazione completa dei dati sensibili e giudiziari e delle relative operazioni, si fa espresso riferimento alla normativa che prevede gli obblighi o i compiti, in base alla quale è effettuato il trattamento e, nel caso specifico, al "**Regolamento recante identificazione dei dati sensibili e giudiziari trattati e delle relative operazioni effettuate dal Ministero della Pubblica Istruzione, in attuazione degli articoli 20 e 21 del decreto legislativo 30 giugno 2003 n.196 recante "Codice in materia di protezione dei dati personali" (Decreto 7 dicembre 2006, n. 305 del Ministero della Pubblica Istruzione)**. Viene recepito anche il provvedimento del Garante del 27/11/2008, così come modificato da quello del 25/06/2009, relativamente agli **Amministratori di Sistema**.

Struttura di riferimento

Tutti i dati posseduti dalla scuola vengono trattati presso gli Uffici della sede dell'Istituto (presidenza, vicepresidenza, ufficio della D.S.G.A., segreterie: personale docente e ATA, alunni; sala docenti, archivi) e confluiscono nel server locale, al primo piano dell'edificio di largo Volumnia ,11. L'Istituto è dotato di un server, utilizzante il sistema operativo Windows Server 2003. Nessuna altra struttura concorre al trattamento dei dati in possesso dell'Istituto, ad eccezione della società Argo Software s.r.l. di Ragusa e degli amministratori del sito web Prof.ssa Donatella Giordano (animatrice digitale) e Prof.ssa Laura Riccardi (vicepreside). L'istituto utilizza, previo contratto con la società Argo Software s.r.l., fornitrice del servizio e relativo software, il servizio Argo Db, che consente di eseguire automaticamente copie di back-up dei propri dati e di conservarle, sia in tempo reale sul proprio server locale, una volta al mese, in ora prefissata, via internet, su un server esterno di ArgoSoftware, in modalità criptata. Tutti gli altri dati vengono salvati, previa criptazione, su server remoto di Argo, tramite rete. Inoltre è presente il servizio ArgoScuolanext, tramite il relativo software, che si riferisce al sistema informatizzato con cui far interagire docenti, studenti e famiglie in tempo reale, tramite la rete internet, con crittografia. L'istituto possiede anche un sito web accessibile da internet, ove sono pubblicate notizie riguardanti la didattica, foto di alunni e docenti per le quali vengono acquisite le relative autorizzazioni, nominativi, elenchi e graduatorie, preventivamente "ripuliti" dei dati personali.
Nel sito web della Scuola è presente la sezione **Amministrazione Trasparente**. In questa sezione sono raccolte le informazioni che le Amministrazioni Pubbliche sono tenute a pubblicare nel proprio sito internet nell'ottica della trasparenza, buona amministrazione e di prevenzione dei fenomeni della corruzione (L.69/2009, L.213/2012, D.lgs. 33/2013, L.190/2012). A norma del citato D.lgs. 33/2013 si provvede, in detta sezione, a rendere non intelligibili i dati personali non pertinenti o, se sensibili o giudiziari, non indispensabili rispetto alle specifiche finalità di trasparenza della pubblicazione. Per quanto riguarda la disciplina, in materia di sicurezza e trattamento dei dati, per l'utilizzo dei servizi di Posta Elettronica ed accesso ad Internet, si prende atto del "Disciplinare interno per l'utilizzo dei servizi di Posta Elettronica ed accesso ad Internet, erogati dal Sistema Informativo del Ministero della Pubblica Istruzione" predisposto dalla Direzione Generale per i Sistemi Informativi del Ministero della Pubblica istruzione, in riscontro alle prescrizioni del Garante, con provvedimento generale pubblicato nel Bollettino n. 81 del marzo 2007 e successivamente sulla Gazzetta Ufficiale – Serie generale, n. 58 del 20/03/2007.

Descrizione degli strumenti elettronici utilizzati

Computer, collegati in rete e non, forniti di software Explorer o altri browser, per l'accesso ad Internet. Fax per ricezione/trasmissione di documenti cartacei, che vengono registrati in memoria, ubicato nel locale della segreteria. Nell'edificio sono presenti, nei locali delle segreterie, n° 7 computer desktop e un server sito nella stanza dell'ufficio Alunni con password protetta ed a conoscenza del Dirigente scolastico, e DSGA ,stanza provvista di porta metallica con chiusura a chiave. I PC sopra menzionati, utilizzati per il trattamento dei dati sono tutti collegati in rete locale ed alla rete internet, ma non con gli altri computer della scuola che poggiano su altra lan e linea telefonica diversa. Un altro computer desktop è situati nel locale del Dirigente Scolastico, altri Tre sono presenti in vicepresidenza, Un pc desktop ancora in sala professori.

Banca dati

Tutti i dati contenuti in documentazione cartacea vengono raccolti e conservati nelle segreterie dell'istituto, classificati e custoditi in appositi schedari all'interno di armadi metallici o cassettiere, chiusi e dotati di serrature o lucchetti. I dati relativi al personale, agli alunni ed alla gestione economico-contabile, anche con riferimento all'identità dei fornitori e degli esperti esterni, sono trattati mediante elaborazione elettronica, con appositi software, nei computer degli uffici delle segreterie e da questi trasferiti al server locale in tempo reale. Vengono eseguiti automaticamente copie di back-up dei propri dati e di conservarle su server remoto. I dati personali di anni precedenti, in formato cartaceo, sono sistemati negli archivi.

Luogo di custodia dei supporti di memorizzazione

Tutti i dati vengono custoditi presso gli uffici del DSGA; si trovano memorizzati nel server, dove vengono trasferiti in tempo reale i dati trattati da tutti gli uffici, negli elaboratori degli uffici delle segreterie, del Dirigente Scolastico, vicepresidenza e della D.S.G.A. Copie di backup sono custodite nel server locale e nel N.A.S. del D.S.G.A. e presso i server della società ArgoSoftware s.r.l. di Ragusa, Responsabile esterno del trattamento dei dati, per la realizzazione di copie di backup dei dati su server remoto e l'applicazione Argo Scuolanext. I supporti informatici per le copie di sicurezza ed ogni altro supporto rimovibile, sono custoditi ciascuno nelle stanze dove sono ubicati, le cui porte vengono chiuse a chiave dal personale ATA alla chiusura dell'Edificio scolastico. I dati cartacei sono custoditi in armadi e cassettiere dotati di serrature, posti negli uffici delle segreterie, del Dirigente Scolastico e del D.S.G.A

. Nei cinque locali dell'archivio storico (situati nei seminterrati dei plessi) sono custoditi, in forma cartacea, dati personali di anni precedenti, in armadi e scaffalature; sono escluse le documentazioni contenenti dati sensibili. I locali sono dotati di sistemi di chiusura con serrature o lucchetti.

Tipologia di dispositivi di accesso e modalità di accesso ai dati

Gli strumenti utilizzati per il trattamento sono pc, collegati in rete locale e non. L'accesso agli uffici è consentito solo al personale addetto specificamente incaricato. **Periodicamente, e comunque almeno annualmente**, si verifica la sussistenza delle condizioni per la conservazione dei profili di autorizzazione degli incaricati al trattamento, **conferendo e aggiornando le relative nomine**. *(Regole: 13., 14., 15.)* Il controllo degli accessi alle varie postazioni di lavoro viene effettuato mediante l'istituzione di un sistema di autenticazione che permette l'identificazione indiretta del soggetto autorizzato al trattamento dei dati. *(Regola 1.)* Tutti i computer presenti negli uffici sono bloccati da distinti codici identificativi di accesso tramite riconoscimento di una credenziale logica costituita da un codice identificativo associato ad una password di almeno otto caratteri, di cui sono a conoscenza esclusivamente i singoli addetti incaricati, ai quali il D.S.G.A. affida anche la custodia temporanea delle chiavi di accesso alle serrature degli armadi metallici e cassettiere, dove sono custodite le documentazioni del cui trattamento sono stati singolarmente incaricati. *(Regole: 2., 3., 5.)* Con le istruzioni impartite agli incaricati amministrativi è prescritto, fra l'altro, di adottare le necessarie cautele per assicurare la componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ad uso esclusivo dell'incaricato. E' prescritto, fra l'altro, agli incaricati, di modificare la parola chiave al primo utilizzo e successivamente almeno ogni tre mesi e di non lasciare incustodito lo strumento elettronico durante una sessione di trattamento. *(Regole: 4., 5., 9., 20., 21.)* E' prescritto che la nuova parola chiave debba essere inserita in una busta chiusa, sigillata e controfirmata sui lembi, da consegnare al Responsabile, che ne curerà la conservazione, per garantire, in caso di assenza prolungata dell'incaricato, l'operatività e la sicurezza del sistema In caso di necessità, il Titolare o il Responsabile hanno la possibilità, previa comunicazione, ove possibile, all'incaricato, di aprire la busta, per esigenze operative o di organizzazione. L'incaricato, in tal caso, provvederà al primo utilizzo a sostituire la parola chiave violata. *(Regola 10.)* E' prescritto agli incaricati amministrativi di conservare separatamente i dati idonei a rivelare lo stato di salute e la vita sessuale, da altri dati personali trattati per finalità che non richiedono il loro utilizzo, trattando i dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, mediante l'utilizzazione di codici identificativi che li rendano temporaneamente inintelligibili, permettendo di identificare gli interessati solo in caso di necessità. E' prescritto che i supporti informatici, già utilizzati per il trattamento dei dati sensibili e giudiziari, possono essere riutilizzati solo se le informazioni precedentemente contenute non sono più in alcun modo recuperabili, dovendo altrimenti essere distrutti. *(Regola 22.)* Per i trattamenti

effettuati, con e senza l'ausilio di strumenti elettronici, è previsto l'aggiornamento periodico, con cadenza almeno annuale, dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative, aggiornando le relative nomine. *(Regola 15.)* Il codice per l'identificazione non può essere assegnato ad altri incaricati, neppure in tempi diversi. *(Regola 6.)* Le credenziali di autenticazione non utilizzate da almeno tre mesi sono disattivate, anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali. *(Regole: 7., 8.)* Viene verificato periodicamente che chi ha accesso a questi dati ne abbia diritto e che tutti gli altri non abbiano accesso agli archivi, anche mediante politiche di sicurezza fisica degli accessi. La scuola utilizza un applicativo (attualmente ArgoSoftware – ArgoScuolanext) che consente il dialogo diretto on-line fra il mondo esterno e i dati che la scuola intende pubblicare o rendere disponibili all'esterno, ai docenti, famiglie e studenti, previa autenticazione e password di accesso. Naturalmente i docenti e le famiglie possono accedere solo ai dati corrispondenti ai propri profili di autorizzazione. L'incarticato del trattamento di dati, Amministrativo dell'Ufficio alunni, gestisce l'attuazione del programma, la distribuzione dei codici di accesso, con le prescrizioni di impiego del servizio. Tutto ciò avviene utilizzando una connessione sicura SSL (Secure Sockets Layer) che prevede che le informazioni su internet viaggino solo in forma criptata.

Tipologia di interconnessione

I collegamenti tra le varie postazioni delle segreterie sono resi possibili dalla "rete locale" degli uffici amministrativi, realizzata mediante cablaggio che consente di raggiungere i vari locali delle segreterie, ove sono le postazioni, dalle quali è, peraltro, possibile accedere ad Internet. Il server e tutti i pc delle varie postazioni delle segreterie, richiedono, all'accensione, le password, prima di avviare i programmi. Le singole postazioni di lavoro condividono con le altre una cartella relative ad operazioni di competenza, non condividono invece quelle di esclusiva competenza di ogni pc. L'attivazione della "condivisione" dei dati contenuti nei pc delle varie postazioni di lavoro delle segreterie collegate in rete è limitata, inoltre, solo alle cartelle che non contengono dati personali. Sono presenti due reti L.A.N. distinte: una per i pc delle segreterie, con server centrale, la seconda separata rete locale, con linea ADSL che interconnette il resto dei laboratori e dei locali della sede dell'istituto, con collegamento ad Internet tramite l'operatore "Telecom Italia", con funzionalità sia cablata che wireless. Il D.S.G.A., Responsabile del trattamento di dati, coordina gli assistenti amministrativi e tecnici nella raccolta, cura, conservazione trimestrale delle parole chiave, nelle attività di verifica di accesso; in caso di relativa nomina, coordina l'Amministratore di sistema delle reti locali, nel back-up mensile, effettuato dal server locale su NAS, per la custodia. Viene, altresì disposto il cambiamento delle password almeno ad ogni trimestre.

Settimanalmente i singoli responsabili sono tenuti a verificare la possibilità di accesso, attraverso i pc e la rete, ai dati. Le parole chiave vengono consegnate dagli incaricati al D.S.G.A. in buste chiuse, controfirmate nei lembi. Analoghe operazioni il D.S.G.A. effettua sul terminale presente nel suo ufficio e di sua competenza, conservandone nell'armadio le parole chiave, in una busta chiusa e controfirmata ai lembi. La parola chiave del server viene fornita e conservata con lo stessa modalità, dal DS, separatamente dalla password locale necessaria per la decriptazione dei dati, nel caso si utilizzi detta funzione. L'istituto dispone di un server, che consente di eseguire copie di back-up dei propri dati e di conservarle, sia in tempo reale sul proprio server locale, per protocollo, personale, inventario e magazzino Tutti gli altri dati vengono salvati, previa criptazione, su server remoto di Argo, tramite rete. Il sistema Argo consente di avere sempre a disposizione i dati conservati, sia in locale, che sul server esterno, per potere effettuare il ripristino del proprio sistema in caso di necessità. Il servizio ArgoScuolanext si riferisce al sistema informatizzato con cui far interagire docenti, studenti e famiglie in tempo reale, tramite la rete internet, con crittografia. I dati della gestione del programma ArgoScuolanext sono trasferiti, previa criptazione, con protocollo SSL (Secure Socket Layer) nei data center presso server farm di Argo che effettua dei back-up automatici e fornisce inoltre un servizio per rendere disponibili alla scuola, ove necessario, dei back-up delocalizzati sul proprio server locale.

Identificativo del trattamento

In questa parte del documento vengono fornite informazioni essenziali in merito alla classificazione dei dati personali trattati, con riferimento alla loro natura; vengono anche indicati i riferimenti relativi alla classificazione ed alla sistemazione e custodia, codificati come nella seguente tabella:

- **Documentazioni**

T01=dati personali relativi agli alunni (registri di classe contenenti le date di nascita, i recapiti delle famiglie e comunicazioni varie, con esclusione di ogni documentazione che possa contenere dati "sensibili"; anagrafe alunni);
T02=dati personali sensibili relativi agli alunni (certificazioni mediche, certificazioni di deficit, diagnosi varie);
T03=dati sensibili relativi ai genitori degli alunni (istanze contenenti dati relativi alla situazione patrimoniale, documentazioni giudiziarie, documentazioni mediche prodotte a corredo delle domande di iscrizione o di altre domande);
T04=dati personali relativi ai dipendenti;
T05=dati personali sensibili relativi ai dipendenti;
T06=dati personali riservati, relativi ad alunni, genitori e personale dipendente, riguardanti corrispondenza riservata custodita dal Dirigente, compresi gli atti relativi ai provvedimenti disciplinari;

T07 =dati personali relativi ai fornitori; dati personali nelle domande di inserimento in graduatorie per incarichi e supplenze di personale docente o A.T.A; dati personali relativi ad esperti esterni;
T08=dati personali di anni precedenti, sistemati negli archivi; sono escluse le documentazioni contenenti dati sensibili.

- **Sede** P01 **– Largo Volumnia, 11 00181 Roma**
- **Stanze**

U01 = Stanza del personale amministrativo (alunni)
U02= Stanza personale amministrativo (gestione personale)
U03= Stanza del D.S.G.A.
U04 = Presidenza
U05 = Stanza Vicepresidenza
U06 = Stanza personale amministrativo (contabilità)
U07 = Sala docenti Tibullo (ingresso via Amulio, 4)

- **Armadi e cassettiere** (dotati di serrature e chiavi di chiusura)

A01 = n°2 armadi metallici , n°2 armadi in legno, n°13 classificatori metallici
A02 = n°1 armadio metallico, n° 4 armadi in legno, n°2 classificatori metallici
A03 = n°4 armadi in legno
A04 = n°4 armadi in legno
A05 = n°4 armadi in legno, n° 1 classificatore metallico
A06 = n°5 armadi metallici, n° 2 classificatori metallici

I dati di tutte le postazioni si trasferiscono in tempo reale sul server locale, custodito nella stanza U01 che ha porte chiuse a chiave alla chiusura dell'istituto, e sul server remoto di Argo, tramite internet.

Dati personali in ingresso

I documenti cartacei in arrivo sono sempre consegnati in busta chiusa al Dirigente Scolastico, che li esamina, destinando al protocollo riservato quelli appartenenti alle tipologie di dati riservati e smistando quelli trattati dagli uffici di segreteria. I documenti consegnati aperti, vengono subito recapitati al Dirigente Scolastico, cui pervengono anche quelli ricevuti tramite FAX. I documenti cartacei sono conservati in armadi o cassettiere, chiusi con apposite serrature.

I dati di tutte le postazioni si trasferiscono in tempo reale sul server locale, custodito in separato locale protetto, e sul server remoto di Argo, tramite internet.

Dati personali in ingresso

- n° 2 computer in U02
- n° 3 computer in U02
- n° 2 computer in U03
- n° 1 computer in U04
- n° 3 computer in U05
- n° 0 computer in U06

- n. 1 server locale, in apposito locale protetto (stanza U01)

Nella scuola sono presenti un laboratorio di informatica, al piano 1° Tibullo, e un laboratorio di informatica piano seminterrato Rodari, ma i loro computer sono utilizzati per la didattica e nessuno di essi contiene dati personali, così come tutti gli altri computer presenti nella nella biblioteca

Plesso scolastico	N° classi	N° alunni	Dir. Sc.	D.S.G.A.	Personale ATA
A/B	64	1160	1	1	25

Gli insegnanti sono complessivamente in numero di 150.

DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITA'

Questa parte del documento contiene una mappa delle strutture con i riferimenti agli incarichi conferiti, ai trattamenti operati ed alle relative responsabilità.

DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITA'

Struttura	**Responsabilità** **Trattamento dati**	**Trattamenti operati**	**Compiti**
1- **Dirigente Scolastico** Prof. **Maria Rosaria Merolla**	**Titolare del trattamento**	Tutti i dati in possesso.	Direzione generale di tutte le attività; gestione delle pratiche riservate.

2 - **D.S.G.A.**	**Responsabile del trattamento**	Tutti i dati riguardanti il personale, docente e A.T.A., gli alunni, le famiglie, gli esperti esterni, i fornitori e trattati dal personale A.T.A.	Coordinamento delle attività amministrative – contabili, con delega di nomina come incaricati, del personale A.T.A., responsabilità sul trattamento di tutti i dati. Coordinamento, se nominato, dell'Amministratore di sistema delle reti locali.
3- **Collaboratori del Dirigente Scolastico**	**Incaricati del trattamento**	Documentazioni riguardanti gli alunni, le famiglie, i docenti e, in caso di impedimento o assenza del Titolare, tutti i dati in possesso, escluse le pratiche riservate.	Supporto organizzativo al D.S., con delega di firma e sostituzione del medesimo in caso di impedimento o assenza. .

Struttura	**Responsabilità** **Trattamento dati**	**Trattamenti operati**	**Compiti**
4 -Soc. **ArgoSoftware s.r.l. di Ragusa**	**Responsabile Esterno del trattamento dati**	Tutti i dati del data base del server locale. Tutti i dati gestiti dalle applicazioni ArgoScuolanext.	Gestione del back up dei dati, dal server locale, sul suo server remoto. Gestione del sistema informatizzato Scuolanext, con cui far interagire docenti, studenti e famiglie in tempo reale, tramite la rete internet.

Struttura	**Responsabilità** **Trattamento dati**	**Trattamenti operati**	**Compiti**
5–**Segreteria Assistenti amministrativi**	**Incaricati del trattamento**	Tutti i dati riguardanti il personale, docente e A.T.A., gli alunni, le famiglie, gli esperti esterni e i fornitori.	Cura di tutte le pratiche amministrative, con particolare attenzione alla tutela della privacy, nella gestione dei dati, per la quale ricevono specifici incarichi, in forma scritta, ed adeguata formazione.

Struttura	Responsabilità	Trattamenti operati	Compiti
6- **Collaboratori scolastici**	**Incaricati del trattamento**	Trattamento occasionale di dati, in occasione dei compiti singolarmente assegnati.	Gestione delle comunicazioni telefoniche e a mezzo fax, della duplicazione attraverso fotocopie, del trasporto documenti e posta e del trasferimento tra i diversi uffici della scuola di domande, documenti ed elenchi contenenti dati personali, nel supporto ai servizi amministrativi, della sorveglianza e vigilanza effettuata sugli alunni.
7-**Docenti e Organi Collegiali Componenti eletti**	**Incaricati del trattamento**	Tutti i dati trattati in fase di elaborazione in uso del registro elettronico Argo ed esecuzione delle delibere dei Consigli di Classe, Collegio Docenti, Consiglio di Istituto, della Giunta Esecutiva e dell'Organo di Garanzia della scuola.	Attività di programmazione e gestione didattica a livello di istituto e di classe. Partecipazione alle attività gestionali; decisioni di tipo amministrativo, finanziario, regolamentare; pratiche disciplinari riguardanti gli alunni ed il personale.

ANALISI DEI RISCHI CHE INCOMBONO SUI DATI

In questa parte del documento vengono individuati i principali rischi potenzialmente pericolosi per la sicurezza dei dati, valutandone la gravità e le conseguenze e ponendoli in correlazione con le misure previste. Sono stati individuati anche degli indicatori di: gravità **G**, probabilità **P**, ed un indice di rischio **I** dell'evento. **G** indica la gravità dell'evento: 1=lievissima; 2=lieve; 3=media; 4=grave **P** indica la probabilità dell'evento: 1=scarsamente probabile; 2= possibilità minima; 3= possibile; 4= probabile **I** indica l'indice di rischio dell'evento: (moltiplicazione dei valori di **G** e **P**)

EVENTO	IMPATTO DI SICUREZZA

Causa	Effetto	**Descrizione**	**Stima del rischio**		
			G	**P**	**I**
Comportamento degli operatori	Accesso agli archivi Accesso al server	Consultazione da parte di non addetti, smarrimento di documenti, diffusione di notizie per violazione del segreto d'Ufficio,	4	1	4
	Distruzione	Distruzione accidentale di documenti.	4	1	4
	Fotocopia non autorizzata	Consultazione da parte di non addetti.	4	1	4
	Errata destinazione	Recapito a terzi di documentazioni contenenti dati personali.	4	1	4
	Mancata chiusura	Accessibilità agli uffici in orari	4	1	4
EVENTO		IMPATTO DI SICUREZZA			
Causa	Effetto	**Descrizione**	**Stima del rischio**		
			G	**P**	**I**

Eventi relativi agli strumenti	Spyware	Duplicazione di dati trasmessi automaticamente da virus che giungono tramite e-mail.	4	1	4
	Virus/Malware	Perdita di dati.	4	1	4
	Intercettazione di informazioni in rete	Accesso ai dati elaborati.	4	1	4
	Malfunzionamento degli strumenti	Impossibilità di accesso ai dati trattati.	4	1	4
Eventi relativi al contesto fisico-ambientale	Allagamento	Infiltrazioni da acqua piovana.	3	1	3
	Incendio	Propagazione di fiamme da cortocircuiti.	4	1	4
	Mancanza di energia elettrica	Danneggiamento di dati a causa dell'improvviso spegnimento dei computer.	4	2	8
	Furto	Sottrazione furtiva di computer e server	4	1	4
	Sovratensioni nella rete elettrica per eventi atmosferici	Danneggiamento componenti attivi nei pc	4	2	8

Indice della gravità di rischio

P4 **I-4** **G1**	**P4** **I-8** **G2**	**P4** **I-12** **G3**	**P4** **I-16** **G4**
P3 **I-3** **G1**	P3 I-6 G2	**P3** **I-9** **G3**	**P3** **I-12** **G4**
P2 **I-2** **G1**	**P2** **I-4** **G2**	**P2** **I-6** **G3**	**P2** **I-8** **G4**
P1 **I-1** **G1**	**P1** **I-2** **G2**	**P1** **I-3** **G3**	**P1** **I-4** **G4**

Fino a **I**-2= indice di rischio lievissimo
I-3 = indice di rischio lieve
Da **I**-4 a *I*-6= indice di rischio medio
I-8 e *I*-9= indice di rischio alto**I**-12 e **I**-16= indice di rischio altissimo

MISURE DI SICUREZZA IN ESSERE E DA ADOTTARE

In questa parte del documento vengono descritte le misure in essere e da adottare per contrastare i rischi individuati a seguito dell'analisi effettuata e della valutazione degli eventi. Per misura viene inteso lo specifico intervento tecnico, informatico od organizzativo, posto o da porre in essere per prevenire, contrastare o ridurre gli effetti relativi ad una specifica minaccia, nonché per ridurre al livello minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta. Vengono indicate, altresì, tutte le attività di verifica e controllo poste o da porre in essere periodicamente, essenziali per assicurare l'efficacia della protezione.

MISURA	RISCHI CONTRASTATI	TRATTAMENTI INTERESSATI	In essere	Da adottare	STRUTTURA OPERATIVA
Istruzioni agli incaricati	Mancata chiusura uffici Accessi agli archivi. Accessi ai	Tutti	x		Dir. Scolastico D.S.G.A. Amministratore di

	computer Accesso al server Visione abusiva.				sistema (se del caso) Assistenti amministrativi
Incarichi di responsabilità	Distruzione accidentale. Errata destinazione. Mancata chiusura uffici Accessi ai computer Accesso al server. Perdita dati.	Tutti	x		Dir. Scolastico D.S.G.A. Amministratore di sistema (se del caso) Assistenti amministrativi
Installazione e aggiornamento antivirus, anti spyware, firewall. Back-up periodici	Accessi non autorizzati ai dati informatici. Duplicazione dati (spyware). Perdita dati (virus) .	Tutti	x		D.S.G.A. Assistenti amministrativi. Amministratore di sistema (se del caso)
Istruzioni agli incaricati. Formazione	Danneggiamento dati informatici. Duplicazione dati. Visione. Perdita dati.	Tutti	x		Dir. Scolastico D.S.G.A. Assistenti amministrativi.
MISURA	**RISCHI CONTRASTATI**	**TRATTAMENTI INTERESSATI**	**In essere**	**Da adottare**	**STRUTTURA OPERATIVA**
Potenziamento sicurezza edifici. Estintori Antifurti	Incendio Intrusioni. Furto Danneggiamento componenti attivi nei pc	Tutti	x		Dir. Scolastico D.S.G.A. Assistenti tecnici Collaboratori scolastici
Istituzione di password di almeno 8 cifre e rinnovabili ogni trimestre	Accesso ai dati Informatici.	Tutti	x		Dir. Scolastico D.S.G.A. Assistenti Amministrativi
Installazione ed utilizzo di gruppi di continuità (ad eccezione del server, per tutti i dispositivi informatici e	Danneggiamento, perdita banche dati informatici, per interruzione energia elettrica	Tutti	x		Dir. Scolastico D.S.G.A. Assistenti Amministrativi e tecnici. Vicepresidenza

PDL (server incluso)					
Circolari	Diffusione di dati	Tutti	x		Dir. Scolastico D.S.G.A.

Saranno installati, in tempi brevi, appositi gruppi di continuità, nelle singole postazioni di lavoro delle segreterie, del Dirigente Scolastico e della Vicepresidenza.

Registrazione degli accessi al sistema di basi dei dati, degli Amministratori di sistema

In caso di necessità di accesso al sistema di basi di dati (aperture delle buste con le parole chiave degli incaricati e accesso all'hard disk di back-up dei dati), il D.S.G.A., Responsabile del trattamento di dati, deve preventivamente informarne il Titolare, acquisirne l'autorizzazione e compilare una apposita scheda di accesso, con i riferimenti temporali e la descrizione dell'evento che lo ha generato, da consegnare al Titolare. Dette schede verranno conservate dal Titolare per almeno sei mesi; inoltre, la Responsabile del trattamento di dati deve relazionare al Titolare, con cadenza almeno annuale, circa le attività svolte, relative alle misure organizzative, tecniche e di sicurezza. In caso della relativa nomina, è prescritto all'Amministratore di sistema delle reti locali, di predisporre idonei sistemi di registrazione degli accessi logici (autenticazione informatica) al server ed agli archivi elettronici, all'atto dell'accesso o tentativo di accesso. E' prescritto che le registrazioni (access log) abbiano carattere di completezza, inalterabilità e possibilità di verifica della loro integrità. Le registrazioni debbono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e conservate per un periodo non inferiore a sei mesi. I dati di log vengono memorizzati, almeno ogni sei mesi, su supporti di memorizzazione non riscrivibili, che l'Amministratore di sistema delle reti locali consegna al Responsabile del trattamento o al Titolare, per la loro custodia. In caso della relativa nomina, l'Amministratore di sistema delle reti locali deve relazionare al Titolare, con cadenza almeno annuale, circa le attività svolte, relative alle misure organizzative, tecniche e di sicurezza.

CRITERI E MODALITÀ DI RIPRISTINO DELLA DISPONIBILITÀ DEI DATI

Banca dati

I dati relativi al personale, agli alunni ed alla gestione economico-contabile, anche con riferimento all'identità dei fornitori e degli esperti esterni sono trattati mediante elaborazione elettronica, con appositi software, nei computer degli uffici delle segreterie e del D.S.G.A. e trasferiti al server che ne effettua automaticamente, un back-up interno giornaliero. I computer, collegati in rete locale, trasferiscono in tempo reale i dati al server. Le copie di back-up dei dati trattati da tutte le unità di elaborazione dei vari uffici, effettuate settimanalmente dal server locale, dal D.S.G.A. o, se nominato, dall'Amministratore di sistema delle reti locali, su N.A.S., sono custodite nella stanza del D.S.G.A. Copie di back-up del data base sono pure settimanalmente trasferite tramite la rete internet, previa criptazione, dal server locale
al server remoto della soc. ArgoSoftware s.r.l. di Ragusa, come copie di sicurezza. I dati della gestione del programma Argo Scuolanext sono trasferiti, previa criptazione, con protocollo SSL (Secure Socket Layer) nei data center presso server farm di Argo che effettua dei back-up automatici e fornisce inoltre un servizio per rendere disponibili alla scuola, ove necessario, dei back-up delocalizzati sul proprio server locale. I dati personali di anni precedenti sono sistemati in archivio; sono escluse le documentazioni contenenti dati sensibili.

Criteri e procedure per il salvataggio e il ripristino dei dati

Per combattere il rischio di perdita, in caso di contaminazione dei pc, i dati sono protetti con software antivirus, antispyware, firewall anti intrusione, aggiornati, con collegamento alla rete internet, in tempo reale, dai siti delle società produttrici. Per i pc non collegabili in rete, o per i siti che non provvedono all'aggiornamento automatico, i software antivirus vengono aggiornati manualmente almeno ogni tre mesi. *(Regole: 16., 17.)* I computer, collegati in rete locale, trasferiscono, in tempo reale, i dati al server.
Dal server, con cadenza mensile , si effettua una copia di back-up di tutti i dati, su N.A.S. *(Regola 18.).*
Inoltre i dati vengono salvati anche tramite un back-up totale del data base, sul server locale, tramite il servizio di back up interno, che avviene con cadenza mensile, mentre, con cadenza mensile, vengono memorizzati su piattaforma remota, con trasmissione criptata, tramite la rete internet, al server remoto della società ArgoSoftware s.r.l. di Ragusa, che si occupa del servizio, affidato dall'istituto.
Il servizio consente il recupero dei dati dal server remoto, in caso di perdita degli stessi.

I dati della gestione del programma ArgoScuolanext, trasferiti, previa criptazione, con protocollo SSL (Secure Socket Layer) nei data center presso i server farm di Argo, che effettua dei back-up automatici, sono anche disponibili alla scuola, ove necessario, con dei back-up, operati dall'Amministratore di sistema delle reti locali, delocalizzati sul proprio server, che quindi incorpora anche quelli gestiti dal sistema Scuolanext. La società ArgoSoftware, a tal fine, limitatamente a detti compiti, viene nominata Responsabile Esterno del trattamento dei dati dell'Istituto, dando ad essa espresso compito di adempiere, in riferimento ai dati memorizzati sui suoi server remoti, a tutte le prescrizioni relative al provvedimento del Garante del 27/11/2008, così come modificato da quello del 25/06/2009, relativamente ai suoi Amministratori di sistema. Per ogni PDL o apparecchiatura informatica deve essere organizzata e prevista una "copia immagine" (sistema operativo, programmi di base utilizzati, impostazioni), in modo da ripristinare immediatamente software, dati e configurazioni.

Modalità di custodia delle copie

Le copie di sicurezza del data base del server, prodotte internamente con cadenza mensile, tramite N.A.S. , posizionato nell'ufficio del DSGA (Regola 23.) Un rack a parete serebbe necessario per contenere le apparecchiature di rete e il disco di rete (NAS), preservandoli in un ambiente protetto da accessi non autorizzati.

Struttura o persona incaricata del salvataggio

Il coordinamento delle attività di salvataggio e di conservazione delle copie è affidato al D.S.G.A. *(Regola 18.)*, nella qualità di Responsabile del trattamento di dati. L'effettuazione delle copie settimanali di back up viene realizzata dal D.S.G.A. o, in caso della relativa nomina.

Pianificazione delle prove di ripristino

Mensilmente vengono effettuate le copie di backup di tutti i dati posseduti dalla scuola e viene anche stabilito un piano mensile di verifica della correttezza ed immediata disponibilità di tutte le copie di sicurezza aggiornate effettuate, al fine dell'eventuale ripristino dei dati, in caso di perdita, in un tempo non superiore ai sette giorni. Questa attività di verifica viene svolta dal D.S.G.A., Responsabile del trattamento dei dati *(Regola 18.)* .

PIANIFICAZIONE DEGLI INTERVENTI FORMATIVI

La formazione del personale costituisce elemento fondamentale per la garanzia di efficiente ed efficace funzionamento di ogni struttura organizzativa, ed in particolare rappresenta supporto indispensabile per l'effettiva implementazione delle disposizioni previste dal D.L.vo 196/2003. Viene, pertanto definito il seguente piano degli interventi formativi per l'anno scolastico 2017/2018.

Descrizione dell'intervento	Struttura interessata	Tempi previsti	Personale
Relazione/circolare del Dirigente Scolastico. Presentazione degli incarichi connessi al D.L. 196/2003 e delle disposizioni richiamate.	DSGA Docenti Ass. Amministrativi Assistenti tecnici Collaboratori scolastici	Presumibilmente inizio anno solare 2018	
Formazione del nuovo personale e/o aggiornamento di quello preesistente sull'utilizzo di computer e rischi connessi	DSGA Ass. Amministrativi Ass. tecnici	Presumibilmente inizio anno solare 2018	
Formazione del nuovo personale e/o aggiornamento di quello preesistente per l'adozione di misure di salvataggio dati	DSGA Ass. Amministrativi Ass. tecnici	Presumibilmente inizio anno solare 2018	
Formazione del nuovo personale e/o aggiornamento di quello preesistente per la conservazione e tutela del materiale cartaceo	DSGA Ass. Amministrativi	Presumibilmente inizio anno solare 2018	
Formazione del nuovo personale e/o aggiornamento di quello preesistente per l'uso del sistema di autorizzazione	DSGA Ass. Amministrativi Ass. tecnici	Presumibilmente inizio anno solare 2018	

TRATTAMENTI AFFIDATI ALL'ESTERNO
Descrizione dell'attività "esternalizzata"

L'istituzione scolastica può avvalersi, per lo svolgimento dei propri fini istituzionali o per quelli miranti all'integrazione dei soggetti diversamente abili, della collaborazione di terapisti, psicologi, medici, esperti e specialisti, assistenti igienico-personali, di docenti esperti esterni, così come in occasione di stage aziendali, di tutor aziendali, o altre figure necessarie per l'attuazione degli interventi previsti dall'offerta formativa. Così come, per la normale gestione operativa, può avvalersi di ditte esterne specializzate nella manutenzione o riparazione di sistemi informatici utilizzati per il trattamento dei dati. In particolare, la società ArgoSoftware s.r.l. di Ragusa gestisce, per conto dell'istituto la trasmissione criptata via internet, dal server dell'istituto, del data base dei dati, al fine di memorizzarli su piattaforma remota (server ArgoSoftware), come back-up di sicurezza, per il ripristino, in caso di perdita degli stessi, dovuta a causa accidentale e del servizio ArgoScuolanext che si riferisce al sistema informatizzato con cui far interagire docenti, studenti e famiglie in tempo reale, tramite la rete internet, con crittografia. A tal proposito e limitatamente per questi fini, la società ArgoSoftware s.r.l. viene nominata Responsabile esterno del trattamento dati. E' inoltre prevista dalla normativa la presenza di genitori e alunni in alcuni Organi Collegiali.

Trattamenti di dati interessati

E' escluso, nei limiti del possibile, l'accesso di soggetti esterni a documentazioni contenenti dati sensibili.
Soggetti esterni *(Regola 25.)*

In merito alla possibilità di trattamento di dati personali da parte dei suddetti soggetti, è previsto che:
1) In caso di **manutenzione** delle apparecchiature informatiche contenenti dati, da parte di ditte esterne, i **titolari e gli addetti** devono assumere, anche su base contrattuale, durante le operazioni di manutenzione, le qualifiche, rispettivamente, di "**Responsabili o incaricati**" del trattamento dati, assumendone in proprio gli obblighi di legge relativi. In particolare devono:
a) accettare di essere nominati (dal **Titolare del trattamento**) responsabili o incaricati del trattamento dati;
b) dichiarare essere consapevoli degli obblighi previsti dal D. L.vo 196/2003;
c) impegnarsi ad ottemperare all'obbligo di tutela dei dati personali e di trattarli ai soli fini dell'espletamento dell'incarico ricevuto
d) rispettare le istruzioni specifiche ricevute per la garanzia di sicurezza dei dati;
e) impegnarsi a relazionare periodicamente sulle misura di sicurezza adottate ed

2) In caso di incarichi, a soggetti esterni, di attività inerenti l'offerta formativa, precedentemente citate, nel caso in cui detti soggetti rivestano la qualifica di **Titolari di società**, è previsto che assumano la qualifica di **Responsabili** del trattamento dei dati, assumendone in proprio gli obblighi di legge relativi. In particolare devono:
a) accettare la nomina (data dal **Titolare del trattamento**) a responsabili esterni del trattamento dati;
b) essere consapevoli degli obblighi previsti dal D.L. 196/2003;
c) impegnarsi ad ottemperare all'obbligo di tutela dei dati personali;
d) impegnarsi a rilevare solo i dati strettamente necessari al procedimento richiesto e rientrante nelle funzioni dell'attività, in assenza dei quali non potrebbe essere in grado di svolgere il proprio ruolo, che il servizio pubblico gli affida;
e) impegnarsi a trattarli con le cautele previste, e conservarli per il tempo necessario all'espletamento delle attività, adottando tutti quegli accorgimenti miranti a salvaguardarne la sicurezza. Il trattamento dovrà essere effettuato manualmente o con l'ausilio di apparecchiature automatizzate, informatiche, elettroniche, secondo modalità idonee a garantire la sicurezza dei dati, ai sensi dell'art.31 del DLgs 196/2003 e del relativo allegato B;
f) rispettare le istruzioni specifiche ricevute per la garanzia di sicurezza dei dati;
g) impegnarsi a relazionare periodicamente sulle misura di sicurezza adottate ed informare immediatamente il Titolare del trattamento in caso di situazioni anomale o di emergenze.
h) dichiarare, inoltre, di rivestire la qualifica di **Titolare del trattamento dati della società**, assumendone in proprio gli obblighi di legge.
3) In caso di incarichi, a soggetti esterni, di attività inerenti l'offerta formativa, precedentemente citate, nel caso in cui detti soggetti siano **persone fisiche**, è previsto che assumano la qualifica di **Incaricati** del trattamento dei dati, assumendone in proprio gli obblighi di legge relativi. In particolare devono:
a) accettare la nomina (data dal **Titolare del trattamento**) a incaricati esterni del trattamento dati;
b) essere consapevoli degli obblighi previsti dal D.L. 196/2003;
c) impegnarsi ad ottemperare all'obbligo di tutela dei dati personali;
d) impegnarsi a rilevare solo i dati strettamente necessari al procedimento richiesto e rientrante nelle funzioni dell'attività, in assenza dei quali non potrebbe essere in grado di svolgere il proprio ruolo, che il servizio pubblico gli affida;
e) impegnarsi a trattarli con le cautele previste, e conservarli per il tempo necessario all'espletamento delle attività, adottando tutti quegli accorgimenti miranti a salvaguardarne la sicurezza. Il trattamento dovrà essere effettuato manualmente o con l'ausilio di apparecchiature automatizzate, informatiche, elettroniche, secondo modalità idonee a garantire la sicurezza dei dati, ai sensi dell'art.31 del DLgs 196/2003 e del relativo allegato B;
f) rispettare le istruzioni specifiche ricevute per la garanzia di sicurezza dei dati;
g) impegnarsi a relazionare periodicamente sulle misure di sicurezza adottate ed

4) Relativamente alla partecipazione di **genitori e alunni** agli Organi Collegiali è previsto che assumano la qualifica di **Incaricati** del trattamento, per i dati personali di cui venissero a conoscenza e dei quali venisse effettuato il trattamento, nell'esplicazione della propria funzione.

In tal caso è previsto che:

a) accettino la nomina (data dal Dirigente Scolastico, **Titolare del trattamento**) a incaricato esterno del trattamento dati;

b) dichiarino di essere consapevoli degli obblighi previsti dal D.L. 196/2003;

c) si impegnino ad ottemperare all'obbligo di tutela dei dati personali;

d) si impegnino a rilevare solo i dati strettamente necessari al procedimento richiesto e rientrante nelle funzioni dell'attività, in assenza dei quali non potrebbero essere in grado di svolgere il proprio ruolo, che il servizio pubblico gli affida;

e) si impegnino a rispettare le istruzioni specifiche ricevute per la garanzia di sicurezza dei dati;

f) si impegnino ad informare immediatamente il Titolare del trattamento in caso di situazioni anomale o di emergenze.

Documento firmato da:
MARIA ROSARIA MEROLLA
29.12.2017 14:49:01 CET

Il Dirigente scolastico
ıria Rosaria Merolla