MINISTERO DELL'ISTRUZIONE DELL'UNIVERSITÀ E DELLA RICERCA ISTITUTO COMPRENSIVO DI RODENGO SAIANO

Scuola primaria e secondaria di primo grado

REGOLAMENTO INTERNO

CONTENENTE LE NORME DI COMPORTAMENTO PER L'ACCESSO E L'UTILIZZO DEI SISTEMI E DELLE RISORSE INFORMATICHE, DELLA NAVIGAZIONE INTERNET, DELLA GESTIONE DELLA POSTA ELETTRONICA NONCHÉ DELLA GESTIONE DEI DOCUMENTI ANALOGICI DELL'ISTITUTO COMPRENSIVO DI RODENGO SAIANO. (all. n. 1 al Regolamento di Istituto del 2018)

Adottato con decreto dirigenziale n. 846/2018 del 29/09/2018
Approvato dal Consiglio d'Istituto con delibera n. 137 del 03/10/2018

Il presente documento ha per oggetto i criteri e le modalità operative per l'accesso ai sistemi ed alle risorse informatiche, per la gestione della navigazione in Internet e della posta elettronica da parte dei dipendenti dell'Istituto Comprensivo di Rodengo Saiano e di tutti gli altri soggetti autorizzati che, a vario titolo, prestano servizio o attività per conto e nelle strutture Istituto Comprensivo.
Il presente documento integra le istruzioni impartite dall'Istituto Comprensivo di Rodengo Saiano in qualità di Titolare del trattamento, in sede di designazione degli incaricati e sostituisce ogni precedente indicazione impartita in materia.

L'utente è responsabile di qualsiasi danno arrecato al Titolare, sia esso patrimoniale che non patrimoniale, e/o a terzi in violazione di quanto espressamente previsto dalla normativa e di quanto indicato nel presente disciplinare. La violazione delle presenti disposizioni può comportare anche l'applicazione delle sanzioni disciplinari rimanendo ferma ogni ulteriore forma di responsabilità penale.
Di seguito, vengono esposte le regole comportamentali da seguire per evitare e prevenire condotte, che anche inconsapevolmente, potrebbero comportare rischi alla sicurezza dei dati, documenti e archivi.

1. UTILIZZO DELLE POSTAZIONE DI LAVORO, SISTEMI PORTATILI, STAMPANTI

1.1 La postazione di lavoro affidata al dipendente deve essere utilizzata strettamente per attività lavorative ed ogni utilizzo differente può contribuire a creare dei disservizi; inoltre, potrebbe insinuare minacce alla sicurezza dei Dati trattati dal Titolare. Tutti i dipendenti devono custodire la propria postazione di lavoro in modo diligente, segnalando per tempo ogni anomalia riscontrata e/o guasto al proprio responsabile o all'Amministratore di Sistema.

1.2 L'accesso a ciascuna postazione è protetto da credenziali di autenticazione che risiedono sul Server di Dominio: tali credenziali sono costituite da "user ID" e "password", e sono conosciute esclusivamente dall'utente.

1.3 Le credenziali di autenticazione devono essere gestite attenendosi alle seguenti istruzioni:

1.3.1 La password deve essere costituita da almeno otto caratteri alfanumerici di cui almeno tre differenti (scelti tra lettere minuscole, maiuscole, numeri e caratteri speciali).

1.3.2 La password deve essere autonomamente sostituita dall'utente (policy impostata lato Server di Dominio) al primo utilizzo e successivamente modificata ogni qual volta sia richiesto dal sistema.

1.3.3 La password non deve contenere riferimenti diretti o indiretti agevolmente riconducibili all'utente stesso.

1.3.4 Le password (anche quelle degli applicativi, i PIN e/o qualsiasi altro codice di protezione) devono essere custodite con la massima attenzione e segretezza (non devono mai essere scritte su fogli o biglietti che vengono lasciati in prossimità del PC) e non devono essere divulgate o comunicate a terzi per nessuna ragione. Saranno passibili di provvedimenti i metodi "non standard" quali post-it, calendari e qualsiasi altro mezzo non idoneo di custodia, che potrà creare un uso illecito delle credenziali.

1.3.5 L'utente è responsabile di ogni utilizzo indebito o non consentito della parola chiave di cui sia titolare.

1.3.6 Le credenziali di autenticazione individuali per l'accesso alle applicazioni non devono mai essere condivise con altri utenti. Se un utente necessita di trattare gli stessi Dati e/o le stesse procedure dovrà richiedere, delle credenziali personali, al titolare del trattamento che a sua volta le chiederà all'Amministratore di Sistema, persona autorizzata a creare le dovute credenziali di autenticazione necessarie.

1.3.7 È fatto divieto di comunicare la password per telefono o altro mezzo a soggetti che si presentano come colleghi, tecnici e supervisori.

1.4 Il dipendente preso atto che, la conoscenza della password da parte di terzi consente agli stessi l'accesso all'elaboratore, l'utilizzo dei relativi servizi in nome dell'utente titolare e l'accesso ai Dati cui il medesimo è abilitato, con possibilità di gestione degli stessi, si impegna a:

1.4.1 non consentire, una volta superata la fase di autenticazione, l'uso della propria postazione di lavoro a personale non autorizzato, in particolar modo per quanto riguarda l'accesso a Internet e ai servizi di posta elettronica;

1.4.2 non utilizzare credenziali (user ID e password) di altri utenti, nemmeno se fornite volontariamente o di cui si sia venuti a conoscenza casualmente;

1.4.3 mantenere la corretta configurazione del proprio PC non alterando le componenti hardware e software predisposte, né tanto meno installando dei software non autorizzati.

1.5 Non utilizzare la funzione, offerta da alcuni software, di salvare automaticamente la password per successivi utilizzi delle applicazioni.

1.6 Non rispondere a messaggi di posta elettronica che richiedano la verifica delle proprie credenziali di accesso ai servizi finanziari (banche o altri istituti finanziari).

1.7 Ogni postazione di lavoro dovrà essere bloccata in caso di non utilizzo o di assenza temporanea, tramite blocco manuale o salvaschermo con richiesta di password al riavvio. Sarà compito del dipendente procedere a tale blocco.

L'Amministratore di Sistema, in ogni caso, imposterà un tempo di 20 minuti come blocco automatico su tutte le postazioni di lavoro.

1.8 In caso di assenza prolungata nel corso della giornata, è fatto obbligo di chiudere le applicazioni aperte dalle quali si ha accesso ai dati personali.

1.9 Spegnere sempre la propria postazione e i relativi dispositivi ad essa connessi al termine dell'orario di lavoro.

1.10 Non è consentito installare/eseguire autonomamente software provenienti dall'esterno senza la preventiva autorizzazione dell'Amministratore di Sistema.

1.11 Nel caso di necessità di acquisto di programmi, di applicativi e procedure di pertinenza esclusiva di uno o più Servizi, sarà necessaria l'autorizzazione preventiva da parte dell'Amministratore di Sistema.

1.12 Non è consentito ai dipendenti modificare le impostazioni sulla scheda di rete LAN e neppure sul browser di navigazione, salvo esplicita autorizzazione dell'Amministratore di Sistema.

1.13 Non è assolutamente consentito l'uso/l'installazione sul proprio PC di dispositivi, neanche personali, di memorizzazione (Hard Disk Esterni, chiavette USB, ecc), comunicazione o altro (masterizzatore, ecc) se non previa espressa autorizzazione dell'Amministratore di sistema, dopo richiesta scritta da parte del soggetto cui è assegnato l'elaboratore.

1.14 In caso di autorizzazione all'utilizzo di supporti di memorizzazione, gli stessi dovranno essere di proprietà del Titolare ed andranno criptati.

1.15 Ogni dipendente deve comunque prestare la massima attenzione ai supporti di memorizzazione di origine esterna onde evitare di scaricare, anche inconsapevolmente, virus e/o qualunque codice maligno.

1.16 È assolutamente vietato copiare, scaricare e mettere a disposizione di altri materiale protetto da copyright (files musicali, filmati, ecc) di cui il Titolare non abbia acquisito i diritti.

1.17 Oltre alle postazioni di lavoro fisse, ogni dipendente autorizzato all'utilizzo di apparecchiature portatili di proprietà del Titolare quali notebook, tablet e smartphone dovrà prenderne particolare cura; le stesse andranno messe in sicurezza creando blocchi di sistema (es: pin, blocco schermo sequenza, sistemi biometrici). L'utente si impegna ad utilizzarle unicamente in prima persona ed infine a restituirle, quando richieste, in buono stato d'uso. In casi smarrimento/perdita di possesso si obbliga ad avvisare tempestivamente (entro 12 ore), in forma scritta, il Titolare del Trattamento e l'Amministratore di Sistema. L'assegnatario si impegna, altresì, a non effettuare alcuna attività illecita per mezzo del bene consegnato ed in particolare: non eseguirà manomissioni fisiche dei dispositivi, non installerà e non accederà a files, materiali, siti o contenuti illeciti ai sensi delle vigenti norme del codice penale o comunque tutelati dal diritto d'autore senza le necessarie licenze.

1.18 Le stampanti verranno installate per gruppi di lavoro, tramite policy di dominio. Per finalizzare la procedura di stampa, andrà inserito un PIN personale al momento del ritiro dei fogli stampati.

1.19 Gli scanner verranno configurati per poter scansionare in cartelle di rete, legate ai gruppi di lavoro. Sarà cura dell'utente cancellare, dalla cartella condivisa, i documenti scansionati una volta verificata l'attività di scansione.

1.20 Non è ammesso l'utilizzo di sistemi/stazioni di lavoro, collegati alla rete interna, che non siano di proprietà Istituto Comprensivo di Rodengo Saiano, a meno che ciò non sia stato preventivamente autorizzato dall'Amministratore di Sistema.

1.21 Qualora dovesse essere consentito l'utilizzo di dispositivi personali, si richiede che anche questi vengano protetti ed in caso di smarrimento/vendita o altra perdita di possesso, si avvisi preventivamente o tempestivamente (entro 24 ore), in forma scritta, il Titolare del Trattamento e l'Amministratore di Sistema.

2. DOCUMENTI INFORMATICI

2.1 I documenti di lavoro andranno salvati esclusivamente negli archivi messi a disposizione dal Titolare (cartelle condivise e/o software gestionali).

2.2 I documenti creati durante le attività lavorative sono di esclusiva proprietà del Titolare, quindi non andranno eliminati se non previa autorizzazione/richiesta.

2.3 La cartella Documenti viene sincronizzata sui server del Titolare ed è di accesso esclusivo dell'utente. In caso di assenza del dipendente, sarà possibile al solo Amministratore di Sistema accedere al contenuto di quella cartella, previa richiesta scritta del Responsabile del Settore. In questo caso, l'utente verrà informato dell'avvenuto accesso.

2.4 In caso di spostamento all'interno della struttura organizzativa, sarà cura del dipendente consegnare al proprio responsabile l'eventuale contenuto della cartella, se contiene informazioni non inerenti al nuovo incarico.

2.5 In ogni caso, non sono ammessi documenti di tipo personale, di qualsivoglia formato (foto, video, ecc). Il Titolare non è responsabile della perdita/alterazione dei suddetti dati se conservati sui propri sistemi.

2.6 Non è consentito l'uso di "cloud", se non espressamente autorizzati dall'Amministratore di Sistema, previa verifica di adeguatezza alla normativa vigente. Il cloud autorizzato è fornito da Google Education di Istituto che garantisce il rispetto delle norme previste in materia di privacy. Di default questi servizi vengono inseriti in "Black List" (vedi ARTICOLO 3).

3. NAVIGAZIONE IN INTERNET

3.1 La postazione collegata ad Internet costituisce uno strumento necessario allo svolgimento dell'attività lavorativa, di conseguenza è proibita la navigazione in Internet per motivi diversi da quelli funzionali all'attività lavorativa stessa.

3.2 Al fine di prevenire rischi di utilizzo improprio della rete reputati non compatibili con l'attività lavorativa, il Titolare utilizza dei sistemi di filtri che impediscono l'accesso diretto a siti non in linea con le finalità del Titolare (black list); questa viene progressivamente implementata e completata.

3.3 L'utilizzo completo di Internet, non filtrato dalla black list, è autorizzato, con richiesta formale all'Amministratore di Sistema, per ciascun utente dal responsabile di Settore.

3.4 Ciascun dipendente è direttamente e personalmente responsabile dell'uso del servizio di accesso ad Internet, dei contenuti che vi ricerca, dei siti che contatta e delle informazioni che vi immette. È vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti online e simili, salvo i casi espressamente autorizzati o attinenti i compiti e le mansioni assegnate e con il rispetto delle normali procedure assegnate.

3.5 È vietata ogni forma di registrazione a siti o mailing list i cui contenuti non siano legati allo svolgimento delle attività lavorative assegnate.

3.6 È vietata la navigazione di siti da cui sia possibile evincere le opinioni politiche, religiose, filosofiche o le abitudini sessuali dell'utilizzatore; non è consentito, inoltre, visitare nè tanto meno memorizzare documenti dal contenuto oltraggioso, discriminatorio che offendono il comune senso del pudore.

3.7 Qualora il programma antivirus installato sul proprio PC riscontri la presenza di un virus, oppure si sospetti la presenza di un virus non rilevato dal programma antivirus, è necessario darne immediatamente segnalazione all'Amministratore di Sistema.

3.8 Non inserire i propri dati di login cliccando direttamente sui link proposti all'interno di un'email, ma digitare l'indirizzo del sito manualmente per essere certi di non incorrere in siti contraffatti (es. phishing).

3.9 Non cancellare la sottoscrizione ad una mailing list di cui non si è certi dell'iscrizione (potrebbe trattarsi di un raggiro da parte di uno spammer per ottenere conferme sulla validità dell'indirizzo email dell'utente).

4. GESTIONE DELLA POSTA ELETTRONICA, PEC E FIRMA DIGITALE

4.1 L'utilizzo della posta elettronica è consentito solo per ragioni di servizio agli utenti identificati con le modalità precedentemente illustrate, ai quali il Titolare assegna una casella email di posta personale e/o di servizio.

4.2 La casella di posta messa a disposizione dal Titolare è uno strumento di lavoro che deve essere quindi utilizzato esclusivamente per esigenze connesse all'attività lavorativa. Non sono ammessi utilizzi diversi o privati dell'indirizzo; conseguentemente i dipendenti ai quali è assegnata sono responsabili del corretto utilizzo della stessa.

4.3 Si evidenzia che, nel caso di trasmissione di dati particolari (art. 9 GDPR) e/o giudiziari (art. 10 GDPR), è opportuno fare ricorso alla crittografia dei documenti.

4.4 È assolutamente vietato:

a. l'utilizzo di posta elettronica istituzionale per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail-list non attinenti all'attività svolta per il Titolare;
b. inoltrare catene telematiche (es. petizioni, giochi) e altre forme di email che non abbiano attinenza con l'attività svolta;
c. utilizzare tecniche di "mail spamming", invio massiccio di comunicazioni a liste di utenti non istituzionali;
d. allegare al testo delle comunicazioni materiale potenzialmente insicuro (programmi eseguibili, macro, script ecc.).

4.5 Dopo la cessazione del rapporto di lavoro, l'account sarà rimosso previa disattivazione. L'account verrà disattivato decorsi quindici giorni dalla cessazione del rapporto: tale periodo servirà ad informare i terzi e a fornire a questi ultimi degli indirizzi alternativi cui rivolgersi per restare in contatto con gli Uffici del Titolare competenti per gli specifici procedimenti/affari.

4.6 In casi di assenza improvvisa o prolungata del dipendente, su richiesta del responsabile competente, l'Amministratore di Sistema potrà accedere al contenuto della casella di posta elettronica al solo fine di recuperare messaggi urgenti per l'attività istituzionale. Di tale accesso viene data immediata notizia al dipendente, con l'invito a modificare la password del proprio account al primo accesso al sistema successivo alla comunicazione.

4.7 È vietato l'utilizzo di caselle di posta personali (es. tiscali, gmail, live, ecc) a meno che non siano state autorizzate dall'Amministratore di Sistema.

4.8 È fatto obbligo al dipendente di controllare la cartella "spam" della propria casella di posta elettronica ogni 30 giorni per verificare se il sistema ha erroneamente catalogato i messaggi ricevuti come "indesiderati".

4.9 Nel caso di mittenti sospetti o messaggi insoliti, per non correre il rischio di essere infettati da virus occorrerà cancellare i messaggi senza aprirli.

4.10 Nel caso di messaggi provenienti da mittenti conosciuti ma che contengono allegati sospetti (file con estensione .exe .scr .pif .bat .cmd), questi ultimi non devono essere aperti.

4.11 L'Istituto Comprensivo di Rodengo Saiano si è dotato di Posta Elettronica Certificata a disposizione dei vari uffici. L'utilizzo di altre PEC non istituzionali non è consentito.

4.12 L'Istituto Comprensivo di Rodengo Saiano mette a disposizione del Dirigente Scolastico la Firma Digitale, ed in caso di necessità anche ad altri dipendenti autorizzati. Questa viene rilasciata dal Funzionario del CED, previa autorizzazione degli organi di vertice e presentazione di Documento di identità valido. Oltre alla conservazione e alla cura, si richiede particolare attenzione alla gestione delle credenziali. Si rammenta che la Firma Digitale è strettamente personale e l'uso da parte di terzi non è consentito, né altresì l'utilizzo al di fuori delle attività strettamente lavorative. È fatto obbligo di custodire adeguatamente le credenziali di firma digitale, in modo che siano unicamente nella disponibilità dei soggetti a cui sono stati assegnati.

5. MONITORAGGIO E TRACCIABILITÀ

5.1 Il Titolare può avvalersi di sistemi di controllo per il corretto utilizzo degli strumenti di lavoro (che consentono indirettamente un controllo a distanza dell'effettivo adempimento della prestazione lavorativa e determinano un trattamento di Dati personali riferiti o riferibili ai lavoratori) esclusivamente nel rispetto di quanto previsto dalle norme vigenti e dai provvedimenti delle competenti Autorità.

5.2 In particolare, il Titolare, nell'effettuare controlli sull'uso degli strumenti elettronici, eviterà un'interferenza ingiustificata sui diritti e sulle libertà fondamentali dei lavoratori, come pure di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata.

5.3 Le comunicazioni effettuate attraverso posta elettronica sono riservate, conseguentemente il contenuto non può in nessun caso essere oggetto di alcuna forma di verifica, controllo o censura da parte del Titolare o da parte di altri soggetti.

5.4 Le attività sull'uso di Internet vengono automaticamente registrate in forma elettronica attraverso i LOG di sistema. Il trattamento dei Dati contenuti nei LOG, può avvenire esclusivamente in forma anonima in modo tale da precludere l'identificazione degli utenti e/o delle loro attività.

5.5 I Dati personali contenuti nei LOG possono essere trattati esclusivamente in via eccezionale nelle ipotesi di seguito elencate:

a. rispondere ad eventuali richieste della polizia e/o dell'autorità giudiziaria;
b. richiesta dell'Amministratore di Sistema, limitatamente al caso di utilizzo anomalo degli strumenti informatici da parte degli utenti di una specifica Area/Settore (rilevabile esclusivamente dai dati aggregati) reiterato nel tempo.

5.6 I Dati contenuti nei LOG sono mantenuti per il tempo strettamente necessario al perseguimento di finalità organizzative, produttive e di sicurezza, comunque non superiore a 180 (centottanta) giorni, e sono periodicamente cancellati automaticamente dal sistema.

5.7 I Dati riguardanti il software installato sulle postazioni di lavoro (senza alcuna indicazione dell'utente che ha effettuato l'installazione) possono essere trattati per finalità di verifica della sicurezza dei sistemi ed il controllo del rispetto delle licenze regolarmente acquistate.

6. DOCUMENTI ANALOGICI

In caso di trattamenti senza l'ausilio di strumenti tecnologici bisogna osservare le seguenti prescrizioni:

6.1 Il dipendente non dovrà lasciare incustoditi i documenti contenenti dati personali a lui affidati per l'esercizio della sua attività.

6.2 Evitare il deposito di questi documenti in luoghi di transito come corridoi o sale riunioni.

6.3 Se la persona designata al trattamento dei dati è costretta ad allontanarsi momentaneamente non deve mai lasciare incustoditi i documenti e gli atti contenenti dati personali e sensibili sulle scrivanie o in altro luogo liberamente accessibile a terzi non autorizzati.

6.4 L'incuria può essere causa di sottrazione di documenti contenenti dati personali o istituzionali con conseguente possibile trattamento illecito; il dipendente è perciò tenuto a rispettare quanto di seguito indicato:

- al termine della sessione di lavoro ricollocare i documenti negli appositi cassetti e contenitori evitando di mantenerli a vista sulla postazione assegnata per tutta la durata dell'assenza;
- usare promemoria volanti solo per indicazioni generiche;
- distruggere i dati cartacei contenenti dati sensibili qualora non debbano essere più utilizzati (es. mediante un trita documenti);
- qualora, per la mansione assegnata, il dipendente tratti abitualmente atti o documenti contenenti dati sensibili dovrà custodirli in armadi chiusi a chiave all'interno di uffici dotati di idonee misure di sicurezza. L'accesso a tali documenti sarà monitorato e consentito solo a coloro che ne sono stati espressamente autorizzati dal loro responsabile;
- qualora, per la mansione assegnata, il dipendente tratti solo accidentalmente atti o documenti contenenti dati sensibili detti dati dovranno essere dallo stesso controllati e custoditi fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione e dovranno essere immediatamente restituiti al termine delle operazioni affidate.

6.5 È severamente vietato utilizzare documenti contenenti dati personali, particolari o giudiziari come carta da riciclo o carta per appunti. Anche al fine di riduzione dei costi, è pertanto opportuno che – in caso di stampa di documenti – i dipendenti utilizzino la modalità "fronte/retro".

GLOSSARIO

AdS: Amministratore di Sistema: Provv. Gen, 27/11/2008 (GU n.300 24/12/2008 e mod. 25/6/2009).
Black List: elenco di siti internet non accessibili da parte degli utenti della rete locale.
Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
Dato particolare: l'art. 9 GDPR definisce come particolari tutti quei dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, i dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
DPO: Data Protection Officer o Responsabile Protezione dei Dati, art.37-39, Reg. UE 2016/679 (GDPR).
GDPR: acronimo di General Data Protection Regulation (in italiano "Regolamento generale sulla protezione dei dati") adottato dal Parlamento europeo e dal Consiglio relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione degli stessi, divenuto pienamente applicabile il 25 maggio 2018.
Incaricati del trattamento dei Dati: non prevedendo espressamente la figura dell'incaricato del trattamento (ex art. 30 Codice), il Regolamento non ne esclude la presenza in quanto fa riferimento a "persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile" (art. 4, par. 10, Reg. UE 2016/679 (GDPR), definizione di «terzo»).
Internet Service Provider: azienda che fornisce il servizio Internet (esempio telecom, tiscali, vodafone).
Log: archivio dei tracciati sulle attività di consultazione in rete locale e non.
Postazione di Lavoro: personal computer collegato alla rete locale tramite la quale l'utente accede ai Servizi ed ai Dati da gestire.
Responsabile del trattamento dei Dati: secondo quanto elencato nell'art. 4, par. 8, Reg. UE 2016/679 (GDPR), per responsabile del trattamento si intende "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento".
Sistemi Portatili: notebook, smartphones e tablet.
Titolare del trattamento: secondo quanto previsto dall'art.4, par. 7, Reg. UE 2016/679 (GDPR) "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali".
Trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.
Utente e-mail (posta elettronica): persona autorizzata ad accedere al servizio di posta elettronica attraverso l'utilizzo di caselle email.
Utente Internet: persona autorizzata ad accedere al servizio di navigazione in Internet.
Violazione dei dati personali: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

ALLEGATO N. 1 AL REGOLAMENTO INTERNO PRIVACY
PROCEDURA PER DATA BREACH

DEFINIZIONI

La presente procedura è adottata dall'Istituto Comprensivo di Rodengo Saiano con sede legale in via Brescia, n.2, 25050 Rodengo Saiano.

Il Titolare del trattamento ha nominato un Responsabile del trattamento (DPO), individuato nello Studio **Vargiu Scuola Srl -** via dei tulipani 7/9 Assemini (CA) E-mail: dpo@vargiuscuola.it.

Ai fini della presente procedura, valgono le seguenti definizioni:

a) Titolare del trattamento: "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri".

b) Responsabile del trattamento: "La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento ai sensi dell'art. 28 GDPR".

c) Incaricato del trattamento: "La persona fisica che nell'ambito della struttura aziendale del Titolare è autorizzata a effettuare attività di trattamento di dati personali".

d) DPO: "Il Responsabile del trattamento come individuato dalla Sezione 4 (artt. 37-39) del Regolamento (UE) n. 2016/679".

e) Dato personale: "Qualunque informazione relativa a persona fisica identificata o identificabile; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, generica, psichica, economica, culturale o sociale".

f) Trattamento: "qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione".

LA GESTIONE DEI DATA BREACH

Ai sensi dell'art. 33 del Regolamento (UE) n. 2016/679, il Titolare del trattamento, in caso sia consapevole di una violazione dei Dati personali trattati, è tenuto: (i) a informare l'Autorità di controllo (il Garante per la protezione dei dati personali, nel caso del territorio italiano) entro e non oltre le 72 ore - preferibile il rispetto del termine delle 48 ore indicato nel Provvedimento del Garante del 2 luglio 2015 allegato - successive all'avvenuta conoscenza della violazione. Si precisa che il Titolare non è tenuto alla notifica se sia

improbabile che la violazione dei Dati personali presenti un rischio per i diritti e le libertà degli Interessati - e, (ii) nel caso in cui tale violazione sia suscettibile di comportare un rischio elevato per i diritti e le libertà degli interessati, a informare senza ritardo anche gli stessi Interessati.

A tal fine, il Titolare del trattamento, come sopra identificato, ha previsto un apposito processo per la gestione e la notifica in caso di Data Breach.

Al fine di rendere effettivo il processo di notifica, è altresì importante che tutti coloro che nell'ambito del rapporto di lavoro e/o di collaborazione trattano Dati personali del Titolare del trattamento siano previamente sensibilizzati e partecipino attivamente a tale processo, segnalando tempestivamente ogni caso di violazione di cui siano venuti a conoscenza e ogni evento che potrebbe potenzialmente condurre ad una violazione.

DATA BREACH E POTENZIALI SCENARI

Il GDPR definisce violazione dei dati personali o Data Breach "*la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati*" (art. 4, n. 12). Le indicazioni di cui alla presente sezione della Procedura valgono per qualsiasi tipologia di Dato personale.

Eventi di Data Breach possono riguardare sia casi cui è connesso un rischio marginale (es. perdita di una chiavetta USB di un dipendente), che casi più critici di furto o perdita di intere basi dati, quali, a titolo esemplificativo, le banche dati gestite dal Titolare del trattamento.
Nel caso si verificasse una delle casistiche riportate di seguito, o un analogo scenario, è fondamentale chiedersi se e quale tipo di Dati personali sono coinvolti nell'evento, e, di conseguenza, procedere alla segnalazione:

- furto o smarrimento di laptop, smartphone, tablet aziendali contenenti Dati personali;
- furto o smarrimento di documenti cartacei contenenti Dati personali;
- furto o smarrimento di dispositivi portatili di archiviazione non criptati, come chiavette USB e hard disk esterni, contenenti Dati personali;
- perdita o modifica irreparabile di archivi contenenti Dati personali in formato cartaceo o digitale (ad esempio, a causa di una errata cancellazione o modifica dai sistemi o dagli archivi digitali aziendali che non possa essere ripristinata attraverso l'uso di un backup);
- diffusione impropria di Dati personali, per mezzo di:
    - invio di e-mail contenente Dati personali al destinatario errato;
    - invio di e-mail con un file contenente Dati personali allegato erroneamente;
    - esportazione fraudolenta o errata di Dati personali dai sistemi aziendali;
- richiesta di invio di documenti e file contenenti Dati personali da parte di un esterno che si finge fraudolentemente un collega, collaboratore e/o altro soggetto e conseguente invio allo stesso di tali documenti e file;
- segnalazione da parte di un fornitore di un evento di Data Breach sui propri sistemi che ha interessato o potrebbe potenzialmente interessare Dati personali del Titolare del trattamento.

PROCESSO DI GESTIONE DEL DATA BREACH

Al fine di consentire una gestione efficace e tempestiva delle violazioni dei Dati personali, il Titolare del trattamento adotta un processo strutturato per la gestione dei casi di Data Breach che prevede:

- Rilevazione e segnalazione del Data Breach;
- Analisi del Data Breach;
- Risposta e notifica del Data Breach;
- Registrazione del Data Breach.

1. Rilevazione e segnalazione del Data Breach

La rilevazione e segnalazione del Data Breach è un obbligo per tutti i dipendenti e/o collaboratori del Titolare del trattamento.

Nel caso in cui si verifichi uno degli eventi sopradescritti descritti o in tutti gli altri casi in cui il soggetto che tratta dati personali sia consapevole di altri eventi potenzialmente rischiosi per i documenti e gli archivi, è tenuto a informare immediatamente il Dirigente Scolastico il quale provvede – senza indugio – a darne notizia al responsabile per la protezione dei dati personali (DPO).

Nel caso di un incidente informatico, dovrà essere compilata scheda su apposito registro informatico la cui struttura è allegata al presente atto (All.1.1). Al registro andranno allegate tutte le comunicazioni relative all'incidente (ad es. denuncia all'autorità giudiziaria, notifica al Garante Privacy e relativa corrispondenza, comunicazioni agli interessati, ecc.).

In tale Registro dovranno essere inseriti tutti gli eventi che determinano o configurano anomalie rispetto alla normale gestione dei sistemi informatici (ad esempio: Virus, perdita di dati, alterazione di dati, attacchi alla rete, furti di credenziali, ecc.).

2. Analisi del Data Breach

A seguito della rilevazione e/o segnalazione, il Dirigente Scolastico – sentito il Responsabile per la protezione dei dati personali - effettua una valutazione al fine di verificare che nell'incidente rilevato siano stati effettivamente violati Dati personali trattati dall'Istituto.

La suddetta analisi è finalizzata alla raccolta ed identificazione delle seguenti informazioni:

- categorie di Interessati cui i Dati personali violati si riferiscono (ad esempio, utenti, dipendenti, fornitori, etc.);
- categorie di Dati personali compromessi (ad esempio, Dati personali, Dati sensibili, Dati giudiziari);
- tipologia di Data Breach: violazione della riservatezza, disponibilità o integrità (ad esempio, accesso non autorizzato, perdita, alterazione, furto, *disclosure*, distruzione, etc.).
- Nell'ambito di tale analisi, il Titolare del trattamento – con il supporto del DPO - identifica le azioni di prima risposta da intraprendere nell'immediato per contenere gli impatti della violazione dei Dati personali.
- Nell'ambito dell'analisi della violazione, vengono identificate anche le seguenti informazioni:
    - identificabilità degli Interessati i cui dati rappresentano l'oggetto della violazione;

- misure di sicurezza tecniche e organizzative che potrebbero aver parzialmente o *in toto* mitigato gli impatti relativi al Data Breach;
- ritardi nella rilevazione del Data Breach;
- numero di individui interessati.

Sulla base dei suddetti parametri, il Titolare del trattamento competente procede alla valutazione della gravità del Data Breach relativamente ai diritti ed alle libertà degli Interessati, a seconda della natura dei Dati personali (ad esempio, Dati Sensibili e/o Giudiziari), delle misure di sicurezza adottate, della tipologia di interessati (ad esempio, minori o altri soggetti vulnerabili).

3. Risposta e notifica del Data Breach

La precedente fase di analisi fornisce al Titolare del trattamento gli strumenti necessari a identificare e valutare le conseguenze negative e gli impatti causati dalla violazione di Dati personali rilevata.

Nel caso in cui dovesse risultare improbabile che il Data Breach presenti rischi per i diritti e le libertà degli interessati, la notifica all'Autorità Garante risulta essere non obbligatoria. Tale valutazione è condivisa con il DPO.

Qualora al contrario dovesse risultare possibile che il Data Breach presenti rischi per i diritti e le libertà degli Interessati, il Dirigente Scolastico, con il supporto del DPO, procedere a predisporre la notifica all'Autorità Garante secondo il modello allegato al presente atto (All.2).

La notifica viene effettuata all'Autorità Garante entro 72 ore dal momento in cui il Data Breach è stato rilevato.

La suddetta notifica contiene almeno le seguenti informazioni:

- ✓ natura della violazione dei dati personali (*disclosure*, perdita, alterazione, accesso non autorizzato, etc.);
- ✓ tipologie di Dati personali violati;
- ✓ categorie e numero approssimativo di Interessati cui i dati compromessi si riferiscono;
- ✓ nome e dati di contatto del DPO, che sarà l'interfaccia per Titolare del trattamento nei confronti dell'Autorità di controllo;
- ✓ probabili conseguenze della violazione dei Dati personali;
- ✓ descrizione delle misure che il Titolare del trattamento ha adottato o è in procinto di adottare al fine di mitigare le conseguenze del Data Breach;
- ✓ ove la stessa non sia presentata entro 48/72 ore dalla rilevazione, i motivi dell'eventuale ritardo nella comunicazione.

Qualora non sia stato possibile fornire contestualmente tutte le informazioni obbligatorie, il Dirigente Scolastico raccoglie quanto prima le informazioni supplementari e provvede a integrare, senza ritardo, la notifica già inoltrata all'Autorità di Controllo.

Oltre a notificare il Data Breach all'Autorità Garante, il Titolare del trattamento è tenuto a valutare l'esigenza di procedere con la denuncia all'Autorità Giudiziaria competente, nonché con la notifica del Data Breach anche ai soggetti interessati i cui dati siano stati violati.

Per stabilire se sia necessario provvedere alla notifica agli Interessati, il Titolare del trattamento, di concerto con il DPO, deve valutare i seguenti fattori:

- ✓ il trattamento può comportare discriminazioni, furto d'identità, perdite finanziare, disturbi psicologici, pregiudizio alla reputazione, perdita di riservatezza dei Dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo;
- ✓ gli Interessati rischiano di essere privati dei loro diritti, delle libertà o venga loro impedito l'esercizio del controllo sui Dati personali che li riguardano;
- ✓ sono trattati Dati personali che rivelano l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi a condanne penali e a reati o alle relative misure di sicurezza;
- ✓ in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali;
- ✓ sono trattati Dati personali di persone fisiche vulnerabili, in particolare minori;
- ✓ il trattamento riguarda una notevole quantità di Dati personali e un vasto numero di Interessati.

La notifica agli Interessati deve, pertanto, avvenire nel caso in cui la violazione di Dati personali presenti un rischio elevato per i diritti e le libertà delle persone fisiche, a meno che non sia verificata almeno una delle seguenti condizioni:

- ✓ sono state applicate adeguate misure tecniche e organizzative per proteggere i dati prima della violazione, in particolare quelle in grado di renderle non intelligibili per soggetti terzi non autorizzati (ad esempio, misure di cifratura);
- ✓ a valle della rilevazione del Data Breach, sono state adottate misure per impedire il concretizzarsi dei rischi per i diritti e le libertà degli Interessati;
- ✓ la notifica del Data Breach a tutti gli Interessati singolarmente comporta uno sforzo sproporzionato rispetto al rischio. In tal caso occorrerà comunque procedere a una comunicazione pubblica o a una misura simile, tramite la quale gli Interessati siano comunque informati con analoga efficacia.

Il Dirigente Scolastico, di concerto con il DPO, valuta di volta in volta, sulla base della tipologia e del numero di Interessati, il canale di comunicazione che appare più opportuno per trasmettere la notifica agli stessi.

In ogni caso la notifica agli Interessati deve contenere quanto meno:

- ✓ nome e dati di contatto del DPO;
- ✓ descrizione delle probabili conseguenze della violazione;
- ✓ descrizione delle misure adottate o che l'Istituto intende adottare per porre rimedio alla violazione e ridurre gli effetti negativi.

4. Data Breach relativo a dati personali trattati in qualità di Responsabile del trattamento

Qualora, a seguito di una segnalazione o nel corso dell'analisi preliminare di cui al precedente paragrafo 4, il Dirigente Scolastico rilevasse che la violazione qualificabile come Data Breach riguarda dati personali di titolarità di un soggetto terzo trattati dall'istituto in qualità di Responsabile del trattamento, procedono a informare senza ingiustificato ritardo il soggetto terzo titolare del trattamento.

Nel dettaglio, la comunicazione al soggetto titolare del trattamento dovrà contenere quanto meno le seguenti informazioni (oltre a quelle eventualmente richieste dallo stesso soggetto terzo titolare del trattamento):

- ✓ Descrizione della natura della violazione dei dati personali comprensiva, ove possibile, di informazioni in merito alle categorie e al numero di Interessati nonché alle categorie e al volume approssimativo di dati personali oggetto di violazione;
- ✓ Nome e dati di contatto del DPO;
- ✓ Descrizione delle possibili conseguenze della violazione;
- ✓ Descrizione di eventuali misure già adottate o di cui si prevede l'adozione per porre rimedio alla violazione di dati personali e per attenuarne i possibili effetti negativi.

La comunicazione, nel testo convalidato dal DPO, sarà inviata al soggetto titolare del trattamento entro 48 ore dall'avvenuta rilevazione della violazione o nel minore termine eventualmente indicato dal soggetto titolare del trattamento.

PRESCRIZIONI PER LA PREVENZIONE DI DATA BREACH

L'Istituto adotta specifiche strategie per prevenire o minimizzare il verificarsi di Data Breach.

In primo luogo, occorre che tutti gli Incaricati del Trattamento siano consapevoli dei Dati personali che trattano attraverso i propri strumenti (anche cartacei) e dispositivi o a cui hanno accesso tramite i sistemi del Titolare del trattamento. A tal fine, la presente procedura viene loro comunicata dal Titolare del trattamento essi dovranno custodire tali Dati personali ed i relativi documenti con cura e in modo responsabile sia all'interno che all'esterno della propria area di lavoro. Si precisa che i soggetti in questione sono già stati istruiti per mezzo di nomina ad Incaricati del trattamento e devono attenersi alle prescrizioni approvate con il Regolamento interno contenente le norme di comportamento per l'accesso e l'utilizzo dei sistemi e delle risorse informatiche, della navigazione Internet, della gestione della posta elettronica nonché della gestione dei documenti analogici dell'Istituto Comprensivo di Rodengo Saiano adottato con decreto del Dirigente Scolastico e ratificato in sede di Consiglio di Istituto.