ISTITUTO COMPRENSIVO "L. LUZZATI"

Piazza Libertà – 17017 MILLESIMO (SV)

Tel. 019/564019-564048 – Fax 019/5600663

ALLEGATO 4

Regolamento piattaforma G-Workspace

Il presente regolamento è stato approvato con delibera del Consiglio di Istituto del

Attuazione delle misure di sicurezza tecniche

Setting del datacenter

La versione *Google Workspace for Education Fundamental* ovvero di tipo "gratuito" non prevede la possibilità di selezionare la regione dei dati o la *data region*.

Nel caso invece sia in uso una versione della piattaforma cosiddetta "*supported edition*" è necessario, in fase di setting, definire la *data region* con posizionamento del datacenter esclusivamente in Europa. Questa impostazione permette di non incorrere nelle problematiche legate al trasferimento dei dati in paesi extra UE aventi sensibilità e normative non allineate al GDPR.

Gestione delle estensioni

Prima di installare le estensioni è necessario verificarne l'effettiva utilità e funzionalità rispetto agli obiettivi didattici. In particolare, è importante evitare di installare estensioni che nelle relative *Privacy policy* o nei Termini di servizio (*Terms of use* o *Use agreement*) riportino la possibilità da parte del fornitore di trattamenti ultronei dei dati personali effettuati, ad esempio, per finalità di marketing o anche di fidelizzazione.

Attuazione delle misure di sicurezza organizzative

Profilazione utenza

I profili di autorizzazione per la piattaforma G-Workspace (di seguito anche solo "piattaforma") devono corrispondere precisamente all'ambito di utilizzo del singolo utente, nel rispetto del principio del "minimo privilegio" al fine di evitare una esposizione ai rischi eccessiva e non funzionale agli obiettivi dell'Istituzione scolastica.

Nel caso di soggetti con sporadiche esigenze valgono comunque le prescrizioni legate al principio del minimo privilegio, ovvero l'Amministratore della piattaforma concede una autorizzazione momentanea necessaria all'espletamento del singolo compito, riportando in breve tempo l'utenza al profilo di autorizzazione originale.

Verifica dell'ambito di autorizzazione

Ad ogni fine quadrimestre e comunque almeno una volta l'anno è effettuata la Verifica dell'ambito di autorizzazione per tutti gli utilizzatori, docenti, tecnici e allievi in modo da disabilitare i soggetti che non hanno più facoltà di accesso alla piattaforma (ad es. personale in quiescenza, fine del contratto, fine ciclo scolastico).

Disabilitazione periodica delle utenze non più utilizzate

I soggetti che non hanno necessità di utilizzo della piattaforma o che non hanno effettuato accessi negli ultimi 6 mesi sono disabilitati, a prescindere dal fatto che siano ancora in servizio o meno. I soggetti con account disabilitato possono richiedere all'Amministratore della piattaforma l'eventuale riattivazione. L'Amministratore della piattaforma prima di effettuare la riabilitazione del soggetto provvede a verificare la sussistenza dei requisiti di accesso e del relativo profilo di autorizzazione.

Cancellazione documentazione non più utile rispetto alla finalità

I documenti di qualsiasi natura non più utilizzati o utilizzabili (ad es. dopo la fine di un ciclo scolastico) conservati negli spazi a disposizione in piattaforma devono essere cancellati; tale disposizione si applica sia ai file relativi a soggetti non più afferenti all'istituzione scolastica che ai soggetti non più frequentanti.

Utilizzo per le sole finalità didattiche

In considerazione dei rischi legati ai possibili utilizzi ultronei dei dati caricati in piattaforma da parte del fornitore e non potendo fare previsioni su cosa sarà fatto domani con tale patrimonio informativo è necessario prestare la massima attenzione alle tipologie di dati caricati in piattaforma avendo cura di evitare l'upload o la condivisione di documentazione contenente dati personali, specie per quanto riguardante i soggetti più vulnerabili.

Non è quindi possibile caricare documenti, elenchi, file, registrazioni che riportino dati personali dei docenti, dei tecnici o degli allievi, tantomeno se relativi a situazioni particolarmente sensibili come informazioni sullo stato di salute, sulla disabilità o su qualsiasi forma di disturbo dell'apprendimento.

Nel caso di necessità di condivisione della documentazione "sensibile" è possibile procedere attraverso la preliminare criptazione dei file, con comunicazione delle chiavi su altro canale, oppure implementando la pseudonimizzazione del nominativo dei soggetti, attraverso l'adozione e identificazione tramite codice univoco o *nickname*, ugualmente condivisi su altro canale.

In tutti i casi, una volta conclusa la fase di condivisione o redazione a più mani del documento, quindi completata la finalità, è necessario procedere con la cancellazione di tutta la documentazione, senza attendere altra procedura o la conclusione del ciclo scolastico.

Navigazione tramite browser anonimo

Il collegamento alla piattaforma deve avvenire attraverso la funzione di *browser anonimo* (*Navigazione in incognito* su Chrome, *InPrivate* su Edge, *finestra anonima* su Mozilla) in modo che risultino comunque limitati i possibili effetti collaterali legati ai cookie o all'autenticazione trasparente.

Criptazione delle informazioni personali eventualmente condivise

La documentazione contenente dati personali di tipo sensibile o relativa a soggetti con particolari condizioni di vulnerabilità personale, economica o sociale possono essere caricate e condivise in piattaforma a patto di procedere ad una preliminare criptazione dei contenuti. In ogni caso non è possibile denominare le cartelle nelle quali sono posizionati tali file con i riferimenti ai singoli soggetti o che possano anche indirettamente ricondurre in qualche modo al singolo allievo o alla famiglia.

La criptazione può essere effettuata con i software di produttività individuale (come MS-Word) tramite salvataggio con password (criptazione AES-256 dalle versioni 2016 e seguenti) oppure tramite applicativi di compressione e criptazione come 7-zip (in Allegato sono riportate le istruzioni per la criptazione di un file o di una cartella).

La chiave di criptazione deve ovviamente essere facile da ricordare e potrebbe essere, ad esempio, composta dalla denominazione della classe e dall'anno scolastico in corso, con altri prefissi o postfissi posti al fine di aumentare il livello di sicurezza mantenendo una certa mnemonicità. In ogni caso, la criptazione non esime dalla definizione di politiche di accesso ristretto alle sole classi di appartenenza al contenitore documentale.

Controlli periodici

L'Istituto, al fine di tutelare il patrimonio informativo e la continuità dei servizi, utilizza delle procedure e dei dispositivi di sicurezza con i quali controlla e monitora, in modalità aggregata, l'attività dei sistemi e indirettamente anche quella degli utilizzatori; tali controlli sono comunque effettuati in forme tali da precludere la possibilità di identificazione dei soggetti. Al fine di poter valutare i livelli di servizio erogati ed effettuare attività di ricerca forense a seguito di eventuali attacchi, tutte le attività dei sistemi e degli utilizzatori sono salvate in appositi registri o file di log, ai quali può accedere solamente il personale autorizzato e specificatamente nominato Amministratore di piattaforma o di Sistema.

L'accesso ai file di log da parte del personale nominato Amministratore di piattaforma o di Sistema può avvenire per attività di normale manutenzione, a seguito di malfunzionamenti o di degradamento dei livelli di servizio, in funzione di specifiche segnalazioni oppure nel caso di richiesta da parte dell'Autorità Giudiziaria.

I controlli sono effettuati evitando ingiustificate interferenze sui diritti e sulle libertà fondamentali degli utilizzatori, avendo cura di tutelare anche i soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata, nel pieno rispetto dei principi di pertinenza e non eccedenza.

La scelta dei criteri di protezione nei sistemi di sicurezza è tesa al giusto equilibrio tra performance e livello di salvaguardia, proporzionale ai rischi connessi con la tipologia di informazioni trattate. In alcuni casi, i controlli possono interferire con l'esperienza dell'utilizzatore di sistemi e servizi informatici, ad esempio con blocchi nella navigazione, accessi non consentiti, segnalazione di attività non permesse. L'utilizzatore di sistemi e servizi informatici è invitato a segnalare all'Amministratore di piattaforma o di sistema gli elementi che ritiene possano essere migliorati (ad es. falsi positivi).

I sistemi di sicurezza sono configurati in modo da prevenire e bloccare operazioni considerate potenzialmente pericolose oppure non direttamente correlate all'attività lavorativa, quali l'upload e/o il download di file o applicativi software aventi particolari caratteristiche, ad esempio dimensionali o di tipologia di contenuti; eventuali eccezioni dovranno essere segnalate all'Amministratore della piattaforma.

L'utilizzatore di sistemi e servizi informatici non deve modificare, aggirare, disabilitare i controlli di sicurezza. Eventuali attività ritenute sospette comporteranno l'immediata disattivazione dell'account di accesso ai sistemi e servizi, fino al blocco del sistema (tale misura è da ritenersi necessaria poiché è impossibile per un sistema automatico stabilire con certezza se il problema è, o meno, riconducibile ad una compromissione, presentandosi come rischio comunque non accettabile per l'organizzazione e non risolvibile con altri mezzi).

L' Amministratore della piattaforma effettua dei controlli a campione di tipo quantitativo e di tipo qualitativo in modo da evidenziare eventuali comportamenti non allineati al presente regolamento e redige specifico verbale riportando data e ora del controllo, nome del soggetto contravventore ed evidenze di non conformità.

I controlli possono riguardare la presenza di file di dimensioni elevate (es. film, vietati per la normativa sul diritto d'autore), file eseguibili o di installazione (per evidenti problematiche di *licensing*) o di contenuto in contrasto con le indicazioni sopra riportate riguardo a criptazione e pseudonimizzazione dei dati personali.

L' Amministratore della piattaforma procede alla comunicazione al Dirigente scolastico che provvede a correggere il comportamento o in *extrema ratio* a cancellare i file non conformi al presente regolamento.

Condotta e utilizzo etico dei servizi e dei sistemi IT

La piattaforma è fornita agli utenti per condurre e supportare la missione dell'Istituto e le connesse attività rivolte alla didattica.

Gli utenti sono responsabili dell'utilizzo della piattaforma in modo eticamente corretto, sicuro, legale e conforme al presente regolamento, tenendo nella massima considerazione i diritti, le libertà fondamentali, la sensibilità delle persone come anche gli obiettivi primari dell'Istituto.

L'utilizzatore di sistemi e servizi informatici è direttamente responsabile di tutte le attività effettuate con gli account di accesso assegnati, con particolare riguardo alle informazioni inviate o richieste, caricate o visualizzate nel personal computer in uso, applicativo software o piattaforma.

All'utilizzatore di sistemi e servizi IT inclusa la piattaforma sono tassativamente vietate le seguenti attività:

a) La creazione o la trasmissione di qualsiasi materiale o documento, in qualsiasi formato, che possa essere ragionevolmente ritenuto offensivo, diffamatorio o osceno;

b) La creazione o la trasmissione di materiale o documento in qualsiasi formato che possa ragionevolmente essere ritenuto suscettibile di molestare, intimidire, danneggiare o turbare qualcuno o qualcosa;

c) La trasmissione non autorizzata di documenti etichettati come confidenziali su canali o sistemi non sicuri;

d) L'invio di dati di tipo sensibile su canali non sicuri;

e) La creazione o la trasmissione di qualsiasi documento non riconducibile alle funzioni o ai compiti di competenza oppure estraneo alle attività dell'Istituto;

f) L'accesso non autorizzato ai sistemi o ai servizi informatici;

g) L'utilizzo a fini personali dei sistemi, dispositivi o servizi forniti dall'Istituto.

Corretto uso delle Credenziali di autenticazione

Le credenziali di autenticazione sono composte da un codice (account utente) facilmente riconducibile al soggetto e da una *password e/o PIN conosciuti al solo utilizzatore*. ***È tassativamente vietato rivelare la propria password*** di accesso alla rete, agli applicativi o servizi disponibili (inclusi le piattaforme regionali o ministeriali), anche a terzi autorizzati. Qualsiasi azione effettuata utilizzando la coppia "account utente e password e/o PIN" sarà attribuita in termini di responsabilità all'utente titolare registrato, a meno di comprovato illecito da parte di terzi.

La *lunghezza minima della password,* in presenza di autenticazione MFA, deve essere di almeno 8 caratteri; considerato che i sistemi di violazione impiegano tempistiche esponenzialmente proporzionali con la lunghezza della password da violare, è necessario considerare almeno 14 caratteri[1] per gli account dei servizi on-line (es. posta elettronica, piattaforme web) e per gli account qualificati amministrazione di sistema non collegati ad un sistema MFA.

Le password non devono essere trascritte; per questo è importante che siano facili da ricordare. È consigliabile utilizzare tecniche di memorizzazione (es. Mi_P1@c3_l4_P1zz@).

È fondamentale utilizzare password diverse per scopi, piattaforme o applicativi diversi. In caso contrario, sussiste il rischio (non remoto) che l'eventuale violazione di un sistema possa comportare effetti indesiderati anche su tutti gli altri sistemi utilizzati, dell'Istituto e personali, riconducibili allo stesso account.

Le password devono essere modificate ad intervalli regolari per ridurre l'eventuale finestra temporale di esposizione e comunque almeno ogni 3 mesi (cd. *Password aging*).

Le password non devono mai far riferimento a termini di senso compiuto poiché già contenute nei dizionari utilizzati dai sistemi di violazione, oppure essere troppo ovvie (es. 'P@ssword').

Le password non devono essere in alcun modo collegate alla vita privata o lavorativa dell'utilizzatore. Sono quindi da escludere i nominativi dei familiari, la data di nascita, il codice identificativo, la targa dell'auto, la squadra del cuore, il soprannome, ecc. (il precedente elenco non è esaustivo).

Le password devono contenere combinazioni di caratteri Maiuscoli, minuscoli, numeri e caratteri speciali (!, £, $, %, &, /, =, ?, §, @, #, …) anche quando non specificatamente richiesto dal sistema utilizzato (*criteri di complessità*).

Le password non devono essere riutilizzate a breve distanza di tempo; la rotazione minima prevista è almeno pari a 5 password diverse consecutive (cd. *Password history*);

Le password degli account di accesso ai sistemi non sottoposti alle politiche di complessità, di invecchiamento o di rotazione impostate nel sistema di autenticazione centrale, devono comunque rispettare le medesime regole, agendo manualmente.

Le password e i PIN non devono essere comunicate a nessuno, per nessun motivo, con nessun mezzo (ad esclusione del primo accesso o primo invio). In caso di problemi di accesso alle risorse fare riferimento al supporto tecnico.

La digitazione delle password deve avvenire in massima sicurezza evitando di mostrare a terzi la sequenza dei tasti premuti, specie se trattasi di allievi. I colleghi impegnati in attività condivise al computer sono tenuti a voltarsi nel caso sia richiesta l'autenticazione al sistema o alla piattaforma software utilizzati.

È vietata la memorizzazione delle password nei browser o tramite applicativi di gestione password (es. Pocket Password) se non direttamente autorizzati/distribuiti dai Sistemi Informativi (nel caso si utilizzi Mozilla Firefox è possibile memorizzare le password nel browser solo nel caso di attivazione della funzione 'Utilizza una password principale' inserendo una password estremamente complessa

[1] Misura minima prevista da AgID - «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)». (17A03060) (GU Serie Generale n.103 del 05-05-2017)

e lunga). Sono comunque esclusi sistemi o applicativi software di memorizzazione delle credenziali nel cloud.

Non utilizzare strumenti web per la generazione o il controllo del livello di sicurezza delle password (utilizzare eventualmente password con costruzione simile al solo fine di verificarne la robustezza).

Per l'invio delle password di criptazione dei file e della documentazione non utilizzare mai lo stesso canale (es. file criptato inviato via posta elettronica e password comunicata a voce, via telefono).

Non seguire le mode del momento, utilizzare acronimi, *pattern* ('CristianoRonaldo$' oppure sempre il primo carattere di ogni parola maiuscolo e un dollaro finale), ripetizioni e sequenze ('11111Paperin0000' oppure 'QWERTY12345') o parole presenti nei dizionari.

Nel caso di perdita (o anche solo del sospetto di perdita) della segretezza della password è necessario:

a) Modificare immediatamente la password in uso (sui sistemi Windows CTRL+ALT+CANC e Cambia password; verificare le modalità per i singoli applicativi software con autenticazione locale);

b) Comunicare l'accaduto al personale tecnico dell'Istituto, al proprio Dirigente scolastico e al DPO per la valutazione della gravità della situazione e l'attivazione delle procedure di emergenza per incidente alla sicurezza, al fine di attivare tutti i controlli e le contromisure del caso.

Nel caso l'utilizzatore sbagli per più di 5 volte l'inserimento della password, l'account è automaticamente disabilitato; per effettuare la riabilitazione dell'account è necessario contattare il supporto tecnico, aprire un ticket o, se presente, utilizzare il sistema di *self-service password*.

Nei casi di particolare emergenza oppure in presenza di comportamenti che possano comportare problemi di sicurezza, l'Amministratore di Sistema è autorizzato alla momentanea disattivazione dell'account e del sistema utilizzato. Risolta la problematica evidenziata sarà cura dello stesso Amministratore di piattaforma ripristinare le precedenti autorizzazioni.

Le richieste di cambiamento o reset password dell'account di accesso ai sistemi dell'Istituto non sono mai inviate tramite e-mail. Eventuali e-mail che richiedano tramite link la modifica della password devono essere marcate come spam e cestinate.

È tassativamente vietato memorizzare account di accesso ai sistemi e servizi dell'Istituto in documenti salvati in sistemi o dispositivi specie se al di fuori del perimetro dell'Istituto e ad accesso pubblico, inclusi sistemi di file hosting (come Google Drive o Dropbox).

Posta elettronica convenzionale

La posta elettronica è uno strumento di comunicazione e deve essere utilizzato soltanto per effettuare corrispondenze legate al servizio svolto nell'Istituto, anche nel caso di account di posta elettronica di tipo nominativo. In nessun caso sono previsti indirizzi di posta elettronica ad uso privato.

La politica di comunicazione con soggetti esterni all'Istituto prevede, specie in ricezione, l'utilizzo preferenziale di indirizzi di posta elettronici condivisi tra più utilizzatori, come ad es. gruppo@<dominio.it>; in tale modalità il messaggio è inviato al relativo gruppo di utilizzatori e non sono necessarie modifiche in caso di *turnover* del personale.

Ogni utilizzo della posta elettronica deve essere effettuato coerentemente con le politiche e le procedure dell'Istituto nel rispetto dell'etica, della sicurezza e in piena conformità alle leggi applicabili.

L'utilizzatore è tenuto a controllare almeno una volta a giorno il proprio account di posta elettronica per verificare l'eventuale arrivo di nuovi messaggi e conseguentemente l'assegnazione di specifici compiti.

La posta elettronica è erogata esclusivamente in modalità web, con accesso tramite browser. Sono tassativamente escluse altre modalità considerate non sicure come client locali di posta elettronica (es. Outlook o Mozilla Thunderbird) sia sui personal computer che sui dispositivi mobili, tablet o smartphone personali (BYOD). Eventuali deroghe dovranno essere autorizzate dal Dirigente scolastico.

La posta elettronica non deve essere utilizzata per la creazione, distribuzione o rilancio di messaggi di disturbo o offensivi, commenti sull'origine razziale o etnica, sulle opinioni politiche, sulle convinzioni religiose o filosofiche, o sull'appartenenza sindacale, sullo stato di salute o sulla disabilità, sul genere, sul colore dei capelli, sull'età, sulla vita o sull'orientamento sessuale della persona. I dipendenti che dovessero ricevere messaggi con queste tipologie di contenuto da qualsiasi dipendente devono segnalare immediatamente la questione al diretto superiore.

La posta elettronica non deve essere utilizzata per inviare messaggi massivi ad una moltitudine di utenti, in particolare per diffondere locandine, inviti o pubblicizzare eventi, prediligendo la pubblicazione sul sito intranet dell'Istituto nella sezione *news* o eventi, a meno di informazioni particolarmente importanti o urgenti, e comunque su specifica autorizzazione del Dirigente scolastico.

L'utilizzatore non può utilizzare la posta elettronica dell'Istituto per inviare documenti contenenti dati personali, specie se di natura particolare, che lo riguardano o che riguardino soggetti terzi.

La posta elettronica ordinaria o e-mail secondo la recente giurisprudenza[2], rispetto a quanto previsto dal Regolamento (UE) 2014/910 eIDAS (*electronic IDentification Authentication and Signature*) e dalle conseguenti modifiche al D.lgs. n. 82/2005 CAD (Codice dell'Amministrazione Digitale) ha validità giuridica e rilevanza probatoria[3], è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità.

Un messaggio di posta elettronica convenzionale inviato allo stesso dominio (@<dominioscuola.it>) ha un livello di sicurezza mediamente elevato; nel caso di invio ad altri domini di posta anche se istituzionali (ministeri, regioni, comuni, ecc.) non è purtroppo garantito il corrispondente livello di sicurezza, equiparabile addirittura alla semplice cartolina postale. Per questo motivo è necessario verificare sempre il destinatario, soprattutto se multiplo, e in particolare il contenuto della comunicazione (testo e allegati) prima dell'invio.

Alla fine della sessione di lavoro è necessario effettuare sempre la disconnessione (log-out) dal sistema di posta.

[2] Sentenze n. 14716/2011 e n. 11402/2016 Tribunale di Milano

[3] Dalla definizione CAD di "firma elettronica: l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica", l'utilizzo delle credenziali di accesso alla casella di posta elettronica vale a qualificare l'utente e costituisce pertanto una firma elettronica semplice, non avanzata né qualificata, ma comunque non giuridicamente irrilevante e sotto il profilo probatorio liberamente valutabile in giudizio

L'indirizzo di posta elettronica non deve essere utilizzato per la registrazione a siti web che non siano in qualche modo legati alle attività svolte dagli utilizzatori intestatari nell'Istituto, anche al fine di limitare lo spam.

Non lanciare mai i link di annullamento alle sottoscrizioni delle e-mail considerate indesiderate (il cd. "*unsubscribe*"), al fine di ridurre il rischio di conferma dell'esistenza e utilizzo della e-mail.

I sistemi di sicurezza attivi come firewall e antispam garantiscono con discreta probabilità che le e-mail consegnate siano esenti da pericoli. È comunque a carico dell'utilizzatore la verifica ultima di:

a) **Mittente**: deve essere conosciuto (da verificare l'indirizzo effettivo e non la semplice denominazione); esempio da evitare e marcare come spam è il mittente service145@mail.145.com;

b) **Link**: i link devono essere verificati prima di essere lanciati anche nel caso appaiano a prima vista del tutto familiari (soprattutto come aspetto grafico) al fine di evitare attacchi di tipo *phishing*; la verifica può essere fatta posizionando il cursore del mouse sul link per visualizzare la reale destinazione (ad esempio evitare di fare click su link del tipo http://amazon.net.ru);

c) **Allegati**: diffidate dei file con estensione multipla o senza estensione o con denominazione estranea alle attività o mansioni svolte abitualmente (es. 'Si allega fattura');

d) **Contenuti**: scrittura con errori grossolani (traduzione da sistemi automatici), riferimenti alla chiusura di un conto o di un servizio, parole come "URGENTE", richieste di dati personali o di password, file che non sono mai stati richiesti o con estensioni sconosciute o sospette.

Nei casi dubbi non aprire le e-mail o gli allegati e contattare il supporto tecnico che provvederà alla verifica secondo le corrette procedure di sicurezza.

È vietato il *forward* o rilancio della posta sui dispositivi mobili (es. smartphone e tablet) personali. Il *forward* dei messaggi è permesso solamente sui dispositivi mobili di proprietà dell'Istituto, agli utilizzatori specificatamente autorizzati.

L'utilizzo di *forward* di posta automatico dell'Istituto su altri sistemi (es. Gmail personale) è vietato; questo al fine di garantire un adeguato livello di sicurezza dei contenuti dei messaggi come, ad esempio, gli allegati contenenti dati personali o riservati inviati dal mittente che, non essendo a conoscenza del rilancio, non adotta le misure necessarie alla protezione dei contenuti prevista per trasferimenti al di fuori dell'Unione Europea.

La posta elettronica fornita dall'Istituto non può essere utilizzata per scopi personali estranei all'attività lavorativa. Viceversa, è vietato utilizzare o fornire e-mail personali per scambiare informazioni, contenuti o allegati connessi all'attività lavorativa.

L'invio di file tramite link ai sistemi di hosting è permesso solo se i file sono criptati e le chiavi di criptazione sono condivise su altro media. Le procedure di criptazione sono riportate in allegato al presente regolamento.

Non consultare la posta elettronica dell'Istituto presso Internet point, Wi-Fi pubblici o sistemi di connettività condivisa (es. alberghi, ristoranti, bar) al fine di ridurre rischi legati all'esfiltrazione delle credenziali.

Eventuali raccomandazioni o indicazioni ricevute via e-mail, anche da soggetti conosciuti, non devono essere seguite poiché nella maggior parte dei casi si tratta di virus di tipo HOAX (cd. bufale). In caso di dubbi contattare sempre il supporto tecnico.

Marcare sempre come spam le e-mail che appaiono come *scam* ovvero tentativi di truffa pianificata con metodi di ingegneria sociale (in genere nella e-mail si promettono enormi guadagni in cambio di somme di denaro da anticipare).

Le e-mail che richiedono l'attivazione delle macro di MS-Word o MS-Excel prima del download degli allegati devono essere immediatamente marcate come spam.

Non attivare mai i link presenti nelle cosiddette e-mail di reset della password, né fornire mai le credenziali di autenticazione per nessun motivo.

Non rispondere e inoltrare e-mail delle cosiddette catene di Sant'Antonio o rispondere alle e-mail di spam.

Gli allegati inviati via e-mail contenti dati personali o riservati devono essere criptati adottando le procedure e le modalità previste in questi casi. La password di decriptazione deve essere comunicata al destinatario con altro mezzo (es. via telefono).

Le e-mail contenenti evidenze di reati penali devono essere prima visionate dal personale tecnico e poi, se del caso, informate le autorità per la presentazione della denuncia; questo al fine di evitare falsi allarmi.

In casi particolari, di emergenza o semplicemente nel caso non si ricevano le risposte nei tempi attesi, è possibile effettuare la cosiddetta *escalation* ovvero l'invio diretto al superiore del primo destinatario. Le comunicazioni in modalità *escalation*, se considerate inutili, espongono il mittente alle sanzioni disciplinari previste.

L'invio a più soggetti di un messaggio di posta elettronica può essere effettuato in "CC" (Carta Carbone) soltanto nel caso di destinatari appartenenti allo stesso dominio di posta (@<dominioscuola.it>); nel caso di invio a più destinatari è FONDAMENTALE utilizzare il "CCN" (Carta Carbone Nascosta) in modo che i singoli non possano in nessun modo venire a conoscenza degli indirizzi degli altri destinatari.

L'invio di messaggi di posta elettronica a sottogruppi numerosi oppure a tutti i destinatari del dominio di posta è riservato al Dirigente scolastico e ai soggetti specificamente autorizzati. Eventuali forzature del sistema potranno essere sanzionate ai sensi del presente Regolamento.

Dopo la cessazione del rapporto di lavoro dell'utilizzatore, i contenuti della casella di posta elettronica sono conservati per ulteriori 30 giorni (senza considerare le tempistiche di *Retention* del sistema di backup) ai soli fini di tutela dei diritti in sede giudiziaria, senza possibilità di accesso se non da parte degli Amministratori del sistema di posta.

In nessun caso è possibile richiedere copia delle e-mail inviate o ricevute poiché relative al patrimonio informativo dell'Istituto e contenenti comunicazioni esclusivamente legate al rapporto di lavoro.

L'utilizzatore del sistema di posta, in caso di sospensione del servizio per ferie o malattia, è tenuto autonomamente all'impostazione del messaggio di risposta automatica delle e-mail e alla richiesta di inoltro ai colleghi oppure al sostituto o diretto superiore.

In caso di assenza dell'utilizzatore intestatario dell'account e-mail e in presenza di specifiche necessità istituzionali di accesso ai messaggi di posta, il diretto superiore può richiedere al personal tecnico l'accesso al singolo messaggio o all'intera cartella, il *forward* momentaneo o definitivo dell'account di posta su altro indirizzo. Di tale attività deve essere redatto apposito verbale e informato il lavoratore interessato alla prima occasione utile.

Nel caso si riceva una e-mail visibilmente contraffatta da un collega, è necessario informare immediatamente il supporto tecnico.

Nel caso in cui la marcatura come 'messaggio indesiderato' di un insieme ricorrente di messaggi di spam non riduca il problema, sono attivabili i cosiddetti filtri personalizzati, in grado di marcare automaticamente tipologie di e-mail indesiderate.

Al fine di contenere lo spazio di memoria del server di posta, in conformità ai principi di minimizzazione dei dati (art. 5, par. 1, lett. c GDPR) e di limitazione della conservazione (art. 5, par. 1, lett. e) GDPR) l'utilizzatore del servizio di posta elettronica provvede alla periodica cancellazione delle e-mail non rilevanti per la propria all'attività lavorativa e didattica.

L'utente deve organizzare la propria casella di posta in modo tale che ci sia una separazione tra l'archivio corrente e quello storico secondo la regola:

Archivio on line
Posta in Arrivo – 2020
2021
2022

I dati meno recenti potranno così essere memorizzati in modo automatico in contenitori a prestazioni meno elevate.

Nel caso di comportamenti anomali del personal computer, evidenziati a seguito dell'apertura di una e-mail, di un click su un link o di un download di un file, è necessario:

a. staccare immediatamente il cavo di rete;

b. lasciare il computer acceso;

c. segnalare immediatamente l'accaduto al personale tecnico e al Dirigente.

I documenti che generano, o fanno parte di processi che hanno valenza amministrativa nonché quelli aventi efficacia esterna rispetto all'Istituto (come determine, delibere, decreti, verbali, circolari e contratti), in quanto documenti di preminente carattere giuridico-probatorio e fondamentali per la gestione dei procedimenti amministrativi, possono essere inviati via posta elettronica soltanto dopo essere stati oggetto di registrazione di protocollo.

I sistemi di posta elettronica convenzionali non consentono di assicurare le dovute caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità prescritte dalla disciplina di settore applicabile alla conservazione digitale. Per tale motivazione la conservazione dei documenti necessari per l'ordinario svolgimento e la continuità delle attività deve essere assicurata utilizzando gli specifici sistemi di gestione documentale, individuando i documenti che nel corso dell'attività lavorativa devono essere via via archiviati con modalità idonee a garantire tali caratteristiche.

La ricezione di eventuali messaggi che rappresentano istanze o dichiarazioni da parte di terzi, presentate nelle modalità, così come previste all'art. 65 del CAD (es. richiesta con allegata copia di un documento di identità), devono essere girate al sistema di protocollo per la dovuta procedura di registrazione e assegnazione.

BYOD (*bring-your-own-device*) - Dispositivi di proprietà personale

I cosiddetti BYOD (*Bring Your Own Device*, letteralmente "porta il tuo dispositivo") possono essere utilizzati soltanto come sistemi isolati non collegati alla rete dell'Istituto, a meno del Wi-Fi con accesso di tipo *guest* (ove presente). I sistemi di monitoraggio effettuano controlli automatici continui e segnalano al personale tecnico eventuali sistemi e dispositivi non catalogati e non autorizzati che abbiano effettuato un collegamento diretto alla rete locale dell'Istituto (LAN). Eventuali sistemi o dispositivi non autorizzati collegati alla rete dell'Istituto saranno bloccati e l'azione sarà considerata attacco al sistema informatico, segnalata alla Polizia Postale e delle Comunicazioni per la denuncia di reato di accesso abusivo a sistema informatico, ai sensi dell'Art. 615/ter del Codice penale.

È severamente vietato il collegamento alla rete dell'Istituto di sistemi o dispositivi non distribuiti ufficialmente dal personale tecnico di Istituto. Il personale che effettuerà il collegamento diretto alla rete dell'Istituto (sono esclusi i Wi-Fi pubblici) sarà soggetto a sanzioni disciplinari. Saranno inoltre addebitati all'utilizzatore eventuali costi di ripristino o ulteriori danni che dovessero originarsi da un collegamento non autorizzato. Rientrano nei dispositivi del presente comma modem, router, switch, dispositivi wireless, Bluetooth o qualsiasi altro dispositivo che possa in qualche modo ampliare la superficie di esposizione e quindi i rischi connessi.

Il collegamento alla rete Wi-Fi pubblica dell'Istituto (ove disponibile) dei dispositivi di proprietà personale come laptop, tablet o smartphone è possibile seguendo la specifica procedura di autorizzazione, registrazione e autenticazione. In tutti i casi è prevista la registrazione delle attività dell'utilizzatore e della navigazione Internet.

In conformità alla normativa vigente in tema di misure di protezione da adottare nelle attività di trattamento e considerata la non appartenenza di questa tipologia di dispositivi al perimetro di sicurezza dell'Istituto, è vietato salvare dati personali raccolti durante le attività lavorative o comunque riferibili all'Istituto sui BYOD, specialmente nel caso di dati di natura particolare.

Al fine di garantire un adeguato livello di sicurezza nell'utilizzo dei BYOD, anche per la sola consultazione delle piattaforme pubbliche (es. posta elettronica), comunque equiparabile a quello stabilito per l'Istituto, è necessario che i tali dispositivi siano dotati almeno di antivirus con basi aggiornate, firewall locale attivo, aggiornamento del sistema operativo e dei componenti, assenza di software copiato o "*crackato*".

In nessun caso è possibile installare sui dispositivi BYOD software con licenza di proprietà dell'Istituto.

Il trasporto al di fuori del perimetro dell'Istituto di dispositivi di memorizzazione personali contenenti dati sensibili per l'Istituto è vietato. Eventuali repliche o copie di sicurezza delle informazioni devono essere autorizzate e tracciate, secondo le procedure previste. La responsabilità in caso di perdita, smarrimento e involontaria diffusione dei dati contenuti nel dispositivo durante il trasporto al di fuori degli uffici, sarà attribuita all'utente titolare registrato.

Nell'ipotesi di smarrimento o furto di un dispositivo BYOD contenente dati personali riconducibili all'Istituto titolare del trattamento dei dati, è obbligatorio comunicare l'accaduto al DPO/RPD per l'attivazione della procedura di incidente alla sicurezza e, nei casi più gravi, di *Data Breach.*

File hosting

Il file hosting di dati personali o riservati, riconducibili all'Istituto su sistemi non forniti ufficialmente dall'Istituto come Google Drive personali, Dropbox, WeTrasfer è vietato.

È possibile utilizzare il sistema di condivisione implementato nel sistema di posta oppure un qualsiasi sistema indicato e fornito ufficialmente dall'Istituzione scolastica secondo le regole sopra riportate.

Eventuali utilizzi di sistemi cloud o di altre piattaforme di condivisione devono essere specificatamente autorizzati dal Dirigente scolastico e comunicata ai tecnici informatici.

Registrazione delle attività (*Accounting*)

A partire dall'accesso ai sistemi o ai dispositivi, le attività degli utilizzatori sono registrate per motivazioni di sicurezza in appositi file detti di *log*. Nei sistemi critici, di particolare rilevanza o di fede privilegiata sono memorizzate tutte le singole attività svolte riportando account utente, indirizzo o nome macchina, ora, data e il dettaglio delle azioni svolte, incluso il protocollo di comunicazione utilizzato.

Al fine di contenere lo spazio necessario, i file di log sono conservati in logica di rotazione, ovvero sono sovrascritti al raggiungimento di una certa data o di una certa dimensione, a meno della cosiddetta prevista *retention* dei sistemi di backup; in ogni caso la conservazione è strettamente limitata al perseguimento delle finalità organizzative, produttive e di sicurezza.

Alcuni file di log (es. log di accesso) sono conservati per almeno 2 anni dall'evento.

L'eventuale prolungamento dei tempi di conservazione è valutato sempre come eccezione, attuabile soltanto in relazione:

a) ad esigenze tecniche o di sicurezza del tutto particolari;

b) all'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;

c) all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'Autorità giudiziaria o della Polizia giudiziaria.

Il connesso trattamento di dati personali è comunque limitato alle sole informazioni indispensabili per perseguire finalità preventivamente determinate ed è effettuato con logiche e forme strettamente correlate agli obblighi, compiti e missione di Istituto.

I controlli di sicurezza di tipo indiretto, così come stabilito dalla disciplina sui controlli a distanza dei lavoratori[4], e i connessi trattamenti di dati personali lecitamente effettuabili dal datore di lavoro, sono comunque configurati in modo graduale, previo esperimento di misure comunque atte a garantire i diritti degli interessati, escludendo attività idonee a realizzare controlli di tipo massivo, prolungato e indiscriminato dell'attività del dipendente stesso.

Amministratori di Piattaforma

Il personale tecnico amministratore della piattaforma ha facoltà di accesso alle informazioni anche senza i vincoli e le protezioni applicate tipicamente ad un utilizzatore di livello standard; per questo motivo è nominato Amministratore di Sistema dal Dirigente scolastico che provvede ad attribuire singolarmente l'ambito di autorizzazione. Sono considerati Amministratori di sistema i tecnici che

[4] Art. 4, l. 20.5.1970, n. 300 – Statuto dei lavoratori, incluse modifiche disposte dall'art. 23 del D.lgs. 151/2015

lavorano a tutti i livelli della catena tecnologica, di solito al di sotto dello strato applicativo inclusi coloro che possono definire e rilasciare credenziali di autenticazione ad altri soggetti.

I principali compiti di un Amministratore di Sistema sono i seguenti:

a) Monitorare l'infrastruttura informatica di competenza attraverso identificando e prevenendo potenziali problemi;

b) Introdurre ed integrare nuove tecnologie negli ambienti esistenti;

c) Installare e configurare nuovo hardware/software sia lato client, sia lato server;

d) Applicare le patch e gli aggiornamenti necessari al software di base ed applicativo, modificare le configurazioni in base alle esigenze dell'Istituto;

e) Custodire le credenziali di super-amministratore per la gestione della piattaforma e dei sistemi di autenticazione e autorizzazione adottati

f) Creare il profilo degli utenti caricando i dati personali strettamente necessari;

g) Creare le unità organizzative ed i gruppi che permettono la gestione degli utenti in modo massivo e per differenti categorie (come, ad esempio, docenti ed alunni) ;

h) Fare in modo che ciascun utente possa visionare o accedere soltanto ai dati ed alle risorse per i quali possiede l'autorizzazione

i) Gestire e tenere aggiornati gli account utente ed i relativi profili di autorizzazione;

j) Prestare assistenza nell'attivazione e configurazione di servizi vari legati alla piattaforma nell'ottica della dematerializzazione e digitalizzazione dei documenti;

k) Pianificare e verificare la corretta esecuzione dei backup e delle repliche;

l) Valutare ciascuna applicazione utilizzata alla luce dei principi di necessità e di minimizzazione fornendo al titolare del trattamento, tutte le informazioni necessarie per decidere sulla sua adozione.

Sanzioni

Le operazioni effettuate in palese non conformità al presente Regolamento, esporranno alle sanzioni amministrative, civili e penali previste dalla normativa vigente.

Il mancato rispetto o la violazione di quanto previsto dal presente Regolamento, tenuto conto del principio di proporzionalità, è perseguibile con i seguenti provvedimenti:

a) Comunicazione dell'illecito al Dirigente scolastico che provvederà all'applicazione di quanto previsto dal Regolamento Disciplinare applicabile al personale dipendente o, nel caso di allievi, in funzione della gravità dei fatti;

b) Comunicazione alle Autorità competenti nel caso di evidenza di reati;

c) Revoca o disabilitazione temporanea delle credenziali di autenticazione o di specifiche autorizzazioni.

Prescrizioni

L'attività di gestione e utilizzo della piattaforma segue le norme del presente Regolamento.

Il presente Regolamento è distribuito a tutto il personale docente, tecnico e agli allievi.

Gli utilizzatori sono informati sul presente Regolamento, pubblicato nella Intranet di Istituto; saranno inoltre fissate annualmente delle sessioni formative e di aggiornamento per i nuovi assunti in modalità frontale o e-learning.

Il personale neoassunto è tenuto alla visione del presente regolamento prima del rilascio delle credenziali di accesso alla piattaforma.

Annualmente ed in base all'innovazione tecnologica o a sopravvenute esigenze sia organizzative che di sicurezza, si provvederà alla revisione del presente Regolamento e alle procedure allegate.

Aggiornamento e revisioni

Gli utilizzatori possono proporre, ove ritenuto necessario, eventuali integrazioni al presente Regolamento.

Le proposte saranno quindi esaminate dai responsabili della fase di revisione con particolare riferimento alle figure di Animatore digitale e DPO.

Fatte salve eventuali integrazioni normative o provvedimenti delle Autorità, il presente Regolamento è soggetto a revisione almeno una volta ogni 3 anni.

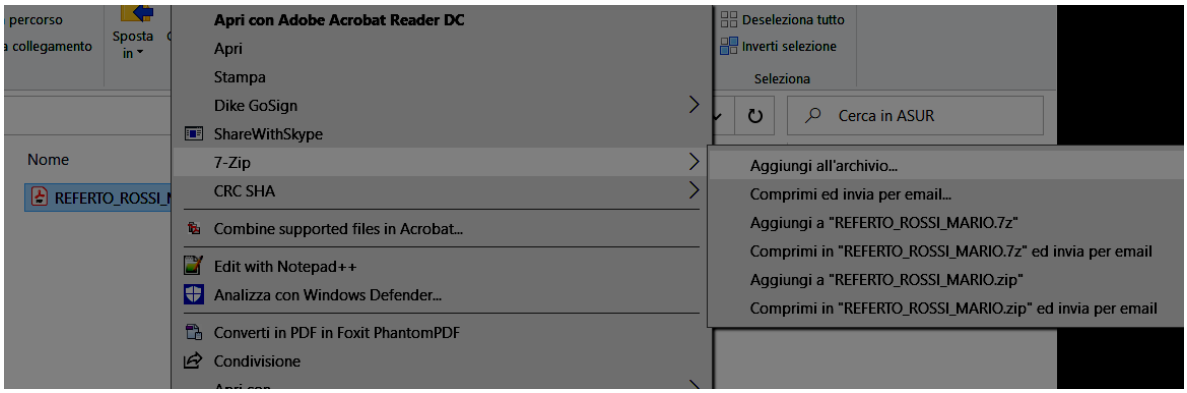
Istruzioni per la criptazione dei file tramite 7-zip

Passo 1: scaricate il pacchetto 7-Zip open source da https://www.7-zip.org/download.html dove sono disponibili i pacchetti per i più diffusi sistemi operativi oppure verificare se già installato sul sistema in uso (nel qual caso è possibile saltare il successivo Passo 2).

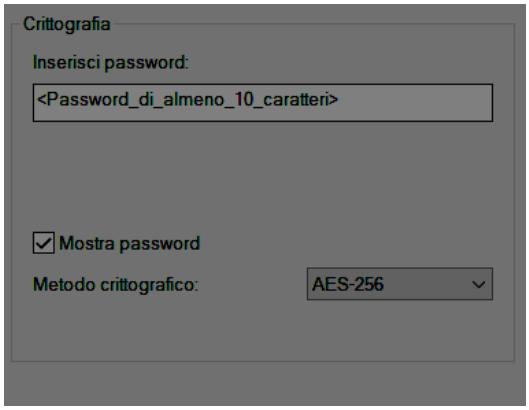
Passo 2: installate 7-Zip; in questo modo, saranno automaticamente integrate le funzioni disponibili nel menu contestuale di Windows Explorer.

Passo 3: selezionate la cartella o il singolo file che desiderate crittografare e fate click con il **tasto destro del mouse**

Passo 4: selezionate "7-Zip" dal menu contestuale e fate clic su "Aggiungi a un archivio..." dal menu pop-up.



Passo 5: inserire la password concordata precedentemente oppure una nuova, da inviare separatamente in una seconda e-mail; la lunghezza deve essere di almeno 10 caratteri e il **Metodo crittografico** di tipo **AES-256**; in questo modo sarà praticamente impossibile ottenere il file senza possedere la chiave.



Passo 6: allegare il file alla e-mail, evitando di riportare nel testo della e-mail ulteriori informazioni

Passo 7: inviare la chiave di decriptazione riportandola nel testo di una seconda e-mail con oggetto identico alla e-mail precedente contenente l'allegato criptato.