Istituto Comprensivo "don Lorenzo Milani"
Via Pietro Mascagni – 20871 Vimercate (MI)
Tel. 039/667522
c.f. 87004970155 – codice univoco UFJXIC
e-mail:mbic8ex001@istruzione.it -mbic8ex001@pec.istruzione.it
www.icsdonmilanivimercate.edu.it
M.I.

- *ALLEGATO 1 AL REGOLAMENTO PIATTAFORMA GOOGLE WORKSPACE FOR EDUCATION* -

NOMINA ED ISTRUZIONI AMMINISTRATORE PIATTAFORMA

E DESIGNAZIONE AI SENSI DELL'ART.2 QUATERDECIS CODICE *PRIVACY (D.Lgs. 196/2003 e ss.mm.ii.),* "Attribuzione di funzioni e compiti a soggetti designati"

IL DIRIGENTE SCOLASTICO,

in qualità di Titolare del trattamento dei dati personali dell'IC Don Milani, Vimercate II,

- VISTO il *Regolamento Generale per la Protezione dei Dati (GDPR)* in merito alle misure di sicurezza minime che ogni Titolare dei dati è tenuto garantire;

- VISTO l'art. 2-quaterdecis del *Codice Privacy* (D.Lgs. 196/2003 novellato dal D.Lgs. 101/2018);

- VISTO il *Provvedimento* del Garante della Privacy del 25/06/2009 in merito all'utilizzo di figure specializzate per la gestione e l'amministrazione delle infrastrutture informatiche;

- PRESO ATTO della necessità di gestire la piattaforma software online scelta dall'istituto per la conduzione di attività a distanza, di seguito denominata "Piattaforma";

- VERIFICATO che l'ambito operativo della Piattaforma non è incluso nelle sfere di competenza dell'Amministratore di Sistema e dell'Amministratore di Rete dell'Istituto;

- VISTO il modello organizzativo relativo alla tutela della *privacy* adottato dall'Istituto, in cui è citata l'opportunità di nominare ed incaricare le figure sopracitate in seno all'organizzazione dell'istituto, qualora reperibili e disponibili;

- TENUTO CONTO delle competenze possedute dalla S.V., con specifico riferimento all'esperienza, capacità e affidabilità richieste dalle vigenti disposizioni per adempiere agli obblighi in materia di sicurezza del trattamento informatico specifico della Piattaforma, già esercitate in qualità di Animatore Digitale dell'Istituto,

NOMINA

la S.V. quale Amministratore della Piattaforma, anche ai sensi dell'art.2-quaterdecis del *Codice Privacy.*

La S.V. accetta tale nomina al fine di potere erogare legittimamente i servizi offerti, e si impegna ad osservare e rispettare, col presente atto, tutte le norme che regolano la materia del trattamento dei dati personali e le istruzioni di trattamento impartite di seguito.

ART. 1 – MISURE TECNICHE GENERALI

In qualità di Amministratore della Piattaforma la S.V. ha la responsabilità di applicare tutte le misure tecniche necessarie alla:

- impostazione dei differenti permessi di utilizzo delle varie APP della *Suite*, con particolare riferimento a quelle che permettono la fuoriuscita dal dominio scolastico (queste ultime vietate per gli studenti a meno di una esplicita autorizzazione da parte degli utenti interessati);

- impostazione dei criteri di sicurezza da assegnare ai dispositivi *tablet android e/o chromebook* da affidare in comodato d'uso;

- creazione, modifica o cancellazione delle unità organizzative gruppi di utenza;

- creazione, attivazione, disattivazione, modifica o cancellazione degli *account* utente;

- suddivisione degli utenti nei vari gruppi/unità organizzative, anche in relazione alle misure di sicurezza impostate;

- attivazione delle procedure di recupero *password* per gli utenti che ne facessero esplicita richiesta (con l'obbligo, in questi casi, di rendere necessario, per l'utente, il cambio della *password* al primo utilizzo);

- risoluzione di problematiche tecniche bloccanti;

- azzeramento dei dati a fine anno scolastico.

Sono escluse le attività di mero supporto tecnico agli utenti.

ART. 2 – MISURE TECNICHE SPECIFICHE E OBBLIGATORIE

Si sottolineano alla S.V. alcune impostazioni da implementare in osservanza dei principi di minimizzazione del trattamento dei dati personali e di utilizzo dei soli dati pertinenti e non eccedenti:

- Richiedere solo nome e cognome dell'utente, unici dati essenziali all'attivazione dell'*account*.

- Disattivare l'autenticazione a due fattori con SMS: questa richiederebbe di memorizzare il numero di telefono dell'utente, azione esplicitamente vietata.

- Controllare le impostazioni e attivare solo le *app* essenziali (*Gmail, Meet, Drive* e Calendario).

- Disattivare i servizi *Google* aggiuntivi non autorizzati dal Dirigente Scolastico.

- Disattivare il *Google Marketplace*, ad eccezione dei componenti aggiuntivi autorizzati dal Dirigente Scolastico.

- Disattivare per scelta predefinita l'accesso ad *app* di terze parti ed utilizzare esclusivamente le disposizioni elencate nel seguito per attivare esclusivamente quelle necessarie alle specifiche attività.

POLITICA DI SICUREZZA APP TERZE PARTI

Si forniscono le fonti in ordine di processo:

a) https://support.google.com/a/answer/7281227

b) https://support.google.com/a/answer/13288950?hl=it#zippy=%2Cche-cosa-sono-i-servizi-google-soggetti-a-restrizioni-e-non-soggetti-a-restrizioni.

In sintesi:

A) PRIMO PASSO: verificare di aver impostato in console le impostazioni di accesso in base all'età, indicando che nelle Unità Organizzativa degli Studenti ci sono dei minorenni:

Vi si accede dalla console di amministratore, Voce: Account->Impostazioni account-> ..selezionare le UO (Unità Organizzative) con studenti .... -> Etichetta Età

Selezionare "Alcuni o tutti gli utenti di questo gruppo o di questa unità organizzativa sono minori di 18 anni".

B) SECONDO PASSO: assegnare il permesso per *APP* che richiedono in "Accedi con *Google*" esclusivamente il nome e la email dell'utente.

Obiettivo: Fare in modo che gli utenti identificati come minori di 18 anni possano usare "Accedi con *Google"* per quelle *app c*he richiedono esclusivamente le informazioni di base (nome, *email* ed eventuale immagine del profilo).

Metodo: selezionare nell'impostazione "App di terze parti non configurate per gli utenti identificati come minori di 18 anni" la seguente opzione: "Consenti agli utenti di accedere alle app di terze parti che richiedono solo le informazioni di base necessarie per Accedi con *Google*".

C) TERZO PASSO: proteggere per *default* i dati interni allo *workspace* di Istituto.

Impostare tutti i servizi *Google* nella modalità "Con restrizioni" (in modo tale che questi servizi consentano l'accesso ai dati alle sole APP contrassegnate come Attendibili, negandolo invece alle altre).

D) QUARTO PASSO: Classificare le *APP* terze parti da attivare, privilegiando l'impostazione "con restrizioni".

Nella scheda "Controllo accesso *app*" è possibile accedere alle richieste di accesso alle *app* terze parti.

Queste richieste di accesso possono essere classificate dall'amministratore come segue:

- Con restrizioni (da ritenere l'opzione predefinita, da preferire): gli utenti possono accedere con *Google* a questa *app*, la quale può richiedere l'accesso solo ai dati di *Google* non soggetti a restrizioni. Quindi nel caso dell'istituto, grazie all'impostazione di cui alla lettera C), praticamente ai soli dati a basso rischio.

- Attendibile (da usare solo se necessario e se si conosce la politica di rispetto dei dati da parte del fornitore della *app*): gli utenti possono accedere con *Google* a questa *app* di terze parti, la quale può richiedere l'accesso ai dati di *Google*, sia ai servizi *Google* non soggetti a restrizioni che (attenzione!) a quelli soggetti a restrizioni.

- Bloccato: gli utenti non possono accedere con *Google* all'*app* di terze parti, la quale non può richiedere l'accesso ai dati di *Google*.

ART. 3 – OBBLIGHI DELL'AMMINISTRATORE DELLA PIATTAFORMA

Al designato è vietato comunicare eventuali dati personali di cui venisse a conoscenza durante l'espletamento delle funzioni di Amministratore della piattaforma, se non esplicitamente autorizzato dal Titolare del Trattamento.

E' sempre vietata la diffusione dei dati personali.

Il designato inoltre:

- ha il dovere di custodire le credenziali di accesso di amministrazione alla piattaforma assegnategli, le quali sono da considerarsi personali. In qualsiasi momento potrà modificare le proprie credenziali in modo tale da mantenere alto il livello di sicurezza dell'accesso;

- ha il potere ed il dovere di compiere tutto quanto si renderà necessario ai fini del rispetto e della corretta applicazione delle misure di sicurezza nella custodia e nel trattamento dei dati personali;

- si impegna ad informare prontamente il Titolare del Trattamento di tutte le questioni rilevanti ai fini di legge ed in termini di sicurezza;

- si impegna a non utilizzare i dati trattati e le informazioni acquisite per finalità che non siano strettamente inerenti alla presente designazione e autorizzazione;

- si impegna ad attenersi, in ogni caso, a tutte le istruzioni che saranno impartite dal Titolare del Trattamento.

La presente nomina produce effetti tra le parti per la durata del rapporto in essere tra l'Istituto e la S.V. o fino a revoca dell'incarico. Gli effetti non cessano con il termine dell'anno scolastico in corso.

Riferimenti del Responsabile per la Protezione dei Dati (DPO) dell'Istituto:

NetSense S.r.l., Partita IVA 04253850871,

email aziendale: info@netsenseweb.com, PEC aziendale: netsense@pec.it

nella persona di: Ing. Renato Narcisi, PEC personale: renato.narcisi@arubapec.it

Il Dirigente Scolastico

Dott.ssa Mariateresa Chieli

documento firmato digitalmente

Vimercate, 17 Aprile 2024

Firmato da:
DIRIGENTE SCOLASTICO
Dott.ssa MARIATERESA CHIELI
17/04/2024 09:44:41