MIM
Ministero dell'Istruzione e del Merito

ISTITUTO COMPRENSIVO
"CAPITANO PUGLISI"
ACATE (RG)

www.icpuglisiacate.edu.it
C.M. RGIC832004 – C.F. 91016750886 - Via Duca D'Aosta, 91 - Tel. 0932/1831960
Email: RGIC832004@istruzione.it – Pec: RGIC832004@pec.istruzione.it

Acate, 26/09/2024

Al prof. Averna Francesco
Al prof. Marino Francesco
Ad Amministrazione Trasparente
– Personale – Incarichi ai dipendenti

NOMINA ED ISTRUZIONI AMMINISTRATORE PIATTAFORMA

E DESIGNAZIONE AI SENSI DELL'ART. 2 QUATERDECIS CODICE PRIVACY

"Attribuzione di funzioni e compiti a soggetti designati"

(documento *allegato al REGOLAMENTO PIATTAFORMA GOOGLE WORKSPACE FOR EDUCATION*)

IL DIRIGENTE SCOLASTICO

- in qualità di Titolare del trattamento dei dati personali dell'Istituzione scolastica (di seguito denominato Istituto);
- visto quanto disposto dal Regolamento Generale per la Protezione dei Dati (GDPR) in merito alle misure di sicurezza minime che ogni Titolare dei dati deve garantire;
- visto quanto previsto dall'art. 2-quaterdecis del Codice Privacy (D.lgs. 196/2003 novellato dal D.lgs. 101/2018);
- visto quanto disposto dal provvedimento Garante 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 privacy dell'istituto, in cui è citata l'opportunità di nominare ed incaricare le figure sopracitate in seno all'organizzazione dell'istituto;
- tenuto conto delle competenze possedute dalla S.V., dopo averne anche verificato l'idoneità rispetto alle caratteristiche di esperienza, capacità e affidabilità richieste dalle vigenti disposizioni per adempiere agli obblighi in materia di sicurezza del trattamento informatico specifico della Piattaforma;

NOMINA

i docenti inseriti tra i destinatari quali Amministratori della Piattaforma, anche ai sensi dell'art. 2-quaterdecis del Codice Privacy.

Le SS.LL. 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 Amministratori della Piattaforma le SS.LL. hanno 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 alle SS.LL. alcune impostazioni da implementare obbligatoriamente, in ossequio ai 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

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 che 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 alla 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:

- **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

Ai designati è vietato comunicare eventuali dati personali di cui venissero a conoscenza durante l'espletamento delle funzioni di amministratori della piattaforma, se non esplicitamente autorizzati dal Titolare del Trattamento.

È sempre vietata la diffusione dei dati personali.

I designati inoltre:

- hanno il dovere di custodire le credenziali di accesso di amministrazione alla piattaforma a loro assegnate, le quali sono da considerarsi personali. In qualsiasi momento potranno modificare le proprie credenziali in modo tale da mantenere alto il livello di sicurezza dell'accesso;
- hanno il potere e 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 impegnano ad informare prontamente il Titolare del Trattamento di tutte le questioni rilevanti ai fini di legge ed in termini di sicurezza;
- si impegnano a non utilizzare i dati trattati e le informazioni acquisite per finalità che non siano strettamente inerenti alla presente designazione e autorizzazione;
- si impegnano 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.

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

Per l'Istituto
IL DIRIGENTE SCOLASTICO
(firma digitale)

Per accettazione
Gli Amministratori della Piattaforma
(firma digitale)

Ministero dell'Istruzione e del Merito

Elenco firmatari

Salvatore Panagia

Firma di Salvatore Panagia

Il 30/09/2024 alle 16:40:51, Salvatore Panagia ha confermato la volonta' di apporre qui la propria Firma Elettronica Avanzata ai sensi dell'art. 20, comma 1-bis del CAD.

Firma .....

Francesco Marino

Firma di Francesco Marino

Il 05/10/2024 alle 15:21:50, Francesco Marino ha confermato la volonta' di apporre qui la propria Firma Elettronica Avanzata ai sensi dell'art. 20, comma 1-bis del CAD.

Firma .....

Francesco Averna

Firma di Francesco Averna

Il 01/10/2024 alle 07:23:33, Francesco Averna ha confermato la volonta' di apporre qui la propria Firma Elettronica Avanzata ai sensi dell'art. 20, comma 1-bis del CAD.

Firma .....