

Registro T1	TRATTAMENTO DEI DATI DEGLI ALLIEVI (AMMINISTRAZIONE DEGLI STUDENTI)		
Sottoregistro A	DIDATTICA DIGITALE INTEGRATA REALIZZATA CON GOOGLE SUITE		
Descrizione sommaria dell'attività di trattamento	In relazione alla Didattica Digitale Integrata (D.D.I.) il trattamento dei dati deve intendersi collegato all'esecuzione di un compito di interesse pubblico di cui è investito l'Istituto, che viene perseguito attraverso una modalità operativa diversa ma che rientra tra le attività istituzionalmente assegnate all'istituzione scolastica ovvero di didattica nell'ambito degli ordinamenti scolastici vigenti.		
Finalità del trattamento	ISCRIZIONE DEGLI ALLIEVI GESTIONE ORGANIZZATIVA DELLA LEZIONE E DELLA VALUTAZIONE DEGLI ALLIEVI TENUTA DEI DATI INERENTI ALLA FREQUENZA SCOLASTICA ED AL RENDIMENTO DEGLI ALLIEVI CERTIFICAZIONI ALLIEVI RISPETTO ALLA LORO FREQUENZA ED AI RISULTATI CONSEGUITI ADEMPIMENTI AGLI OBBLIGHI DI LEGGE CONSERVAZIONE SOSTITUTIVA DEI DATI DI PRESENZA E DI RISULTATO		
Fonte dei dati	Raccolti direttamente presso gli interessati		
	LA TOTALITA' DEI DATI E' RACCOLTA DIRETTAMENTE PRESSO GLI INTERESSATI		
	Raccolti presso terzi		
	MINISTERO E UFFICI SCOLASTICI SUPERIORI RISPETTO A DATI DI NATURA ANAGRAFICA PER FINALITA' ORGANIZZATIVE		
Base giuridica	Dati comuni (art. 6 GDPR)		
	OBBLIGO SCOLASTICO (Legge 296/2006) CONTRATTO (ISCRIZIONE)		
	Dati particolari (art. 9 GDPR)		
	OBBLIGO SCOLASTICO (Legge 296/2006) CONTRATTO (ISCRIZIONE)		
Natura dei dati oggetto di trattamento	Comuni	Termine trattamento	
	DATI ANAGRAFICI DELL'ALLIEVO E DEI SOGGETTI ESERCENTI LA POTESTA'; DATI DI PRESENZA E DI RENDIMENTO SCOLASTICO.	I DATI RELATIVI ALLA DIDATTICA DIGITALE INTEGRATA SARANNO CONSERVATI PRESSO IL FORNITORE PER TUTTA LA DURATA DI PERMANENZA DELL'ALLIEVO PRESSO L'ISTITUTO, DOPO DI CHE, AL TERMINE DELL'ULTIMO ANNO SCOLASTICO DI FREQUENZA, L'ISTITUTO ORDINERÀ AL FORNITORE LA DISTRUZIONE DEI DATI CHE AVVERRÀ ENTRO IL TERMINE TECNICO DI 180 (CENTOTTANTA) GIORNI.	
	Particolari	Termine trattamento	
	NESSUNO	NESSUNO	
	Giudiziari	Termine trattamento	
	NESSUNO	NESSUNO	
Modalità di trattamento dati	I DATI VENGONO TRATTATI IN MODALITA' ELETTRONICA		
Categorie di interessati	ALLIEVI SOGGETTI ESERCENTI LA POTESTA' SUGLI ALLIEVI		
Autorizzati al trattamento	Interni	Trattamenti eseguiti	
	DOCENTI DI CLASSE E DOCENTI DI SOSTEGNO ALLA CLASSE PERSONALE INCARICATO DI PRESTAZIONI DI ASSISTENZA INFORMATICA	RACCOLTA REGISTRAZIONE ORGANIZZAZIONE STRUTTURAZIONE CONSERVAZIONE CONSULTAZIONE ELABORAZIONE SELEZIONE ESTRAZIONE	RAFFRONT UTILIZZO INTERCONNESSIONE BLOCCO COMUNICAZIONE DIFFUSIONE CANCELLAZIONE DISTRUZIONE
	Esterni (Responsabili del Trattamento)	Trattamenti eseguiti	
	PERSONALE INCARICATO DELL'ASSISTENZA INFORMATICA GESTORE DELLA PIATTAFORMA DI DIDATTICA A DISTANZA (GOOGLE)	REGISTRAZIONE ORGANIZZAZIONE STRUTTURAZIONE CONSERVAZIONE CONSULTAZIONE ELABORAZIONE SELEZIONE ESTRAZIONE	RAFFRONT UTILIZZO INTERCONNESSIONE BLOCCO COMUNICAZIONE DIFFUSIONE CANCELLAZIONE DISTRUZIONE
Strutture entro le quali avviene il trattamento dati	Dati in formato cartaceo	Archiviazione storica dati cartacei	
	NESSUNO	NESSUNO	
	Dati in formato elettronico	Archiviazione storica dati elettronici	
	CLOUD (PIATTAFORMA DIDATTICA A DISTANZA)	CONSERVATORIA DIGITALE DI GOOGLE SUITE	
	Software impiegati per il trattamento informatico dei dati in formato elettronico		
GOOGLE SUITE			

Possibili destinatari di attività di comunicazione	Comunicazioni istituzionali	Extra UE	Comunicazioni su base volontaria	Extra UE
	AMMINISTRAZIONE SCOLASTICA	NO	NESSUNO	NO
Informativa	VIENE FORNITA INFORMATIVA SPECIFICA			
Profilazione	NON VIENE ATTUATA NESSUNA ATTIVITA' DI PROFILAZIONE			
Frequenza	IL TRATTAMENTO AVVIENE CON FREQUENZA QUOTIDIANA DURANTE IL PERIODO DI ATTIVITA' SCOLASTICA			
Valutazione del rischio	TRATTAMENTO ANALIZZATO	PROBABILITA' (P)	CONSEGUENZE (C)	LIVELLO DI RISCHIO (LR)
	ATTIVITA' DEI DOCENTI SVOLTA MEDIANTE PIATTAFORMA DIDATTICA A DISTANZA	POCO PROBABILE [2]	LIMITATE [3]	MEDIO BASSO [6]
Valutazione della obbligatorietà della DPIA	L'esito della valutazione dei rischi mostra un livello di rischio ELEVATO per i diritti e le libertà delle persone fisiche interessate ?			NO
	L'attività comporta procedimenti valutativi, di scoring o di profilazione ?			NO
	L'attività comporta la presa di decisioni automatizzate che producono significativi effetti giuridici (ammissioni, assunzioni, concessioni etc.) ?			NO
	L'attività comporta il monitoraggio sistematico di persone fisiche (videosorveglianza ad esempio) ?			NO
	L'attività comporta il trattamento di dati particolari, giudiziari o di natura estremamente personale (es. opinioni politiche) ?			NO
	L'attività comporta il trattamento di dati personali su larga scala ?			NO
	L'attività comporta la combinazione o il raffronto di insiemi di dati derivanti da due o più trattamenti svolti per diverse finalità e/o da titolari distinti, secondo modalità che esulano dal contesto iniziale (big data) ?			NO
	L'attività comporta il trattamento di dati relativi a soggetti vulnerabili (minori, soggetti con patologie psichiatriche, richiedenti asilo, anziani etc.) ?			SI
	L'attività comporta utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative (riconoscimento facciale ad esempio) ?			NO
	L'attività comporta trattamenti che, di per sé, potrebbero impedire agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto (es: screening dei clienti di una banca attraverso i dati registrati in una centrale rischi per stabilire la concessione di un finanziamento).			NO
SI CONCLUDE LA VALUTAZIONE A FAVORE DELLA OPPORTUNITA' (NON OBBLIGO) DI ESEGUIRE LA DPIA PER QUESTO TRATTAMENTO				
Valutazione del rischio su questo trattamento a valle della DPIA	TRATTAMENTO	RISCHIO INTRINSECO (Ri)	VULNERABILITA' (Vu) SI CONSIDERA IL VALORE PEGGIORE	RISCHIO NORMALIZZATO
	ATTIVITA' DEI DOCENTI SVOLTA MEDIANTE PIATTAFORMA DIDATTICA A DISTANZA GOOGLE SUITE	MEDIO BASSO [6]	ADEGUATO [0,25]	BASSO [1,5]

AL FINE DEL CONTENIMENTO DEL RISCHIO SONO ADOTTATE LE SEGUENTI MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE:

MISURA DI SICUREZZA	RISCHIO CONTRASTATO	ADEGUATEZZA (Vu)
Il fornitore e' stato designato come responsabile del trattamento ?	Il contratto concluso con Google Ireland Ltd prevede che il fornitore acquisisca gli obblighi tipici del Responsabile del Trattamenti dei dati come definito all'Art. 28 del GDPR.	ADEGUATO
Il fornitore ha la propria sede all'interno dell'Unione Europea ?	Si la sede di Google Ireland Ltd si trova in Irlanda e conseguentemente lo stesso è soggetto al Regolamento UE 679/2016	ADEGUATO
Quali prodotti sono attivati ?	La suite dispone di diversi servizi integrati, alcuni sono da considerarsi "principali" ed indispensabili per la didattica mentre altri sono aggiuntivi e l'amministratore della piattaforma non deve attivarli salvo richiederne espresso consenso agli interessati.	ADEGUATO
Quali sono i dati acquisiti mediante uso della piattaforma ?	Oltre ai dati essenziali forniti dall'istituto all'atto della creazione delle utenze, l'utilizzo della piattaforma comporta l'acquisizione di informazioni aggiuntive quali: informazioni sul dispositivo (modello, sistema operativo, seriale e numero di telefono dell'utente). Informazioni di registro, attività svolte, informazioni sugli eventi del dispositivo e indirizzo del protocollo internet (IP) dell'utente; Informazioni indirette sulla posizione, come determinato da varie tecnologie tra cui indirizzo IP; e altre informazioni come il numero di versione dell'applicazione e cookie o simili utilizzati per raccogliere e memorizzare informazioni su un browser o dispositivo, come la lingua preferita e altre impostazioni.	ADEGUATO
Come vengono utilizzati questi dati acquisiti ?	Le informazioni personali dell'utente vengono utilizzate solo per fornire i servizi principali sopra descritti. Google si impegna a non pubblicare annunci commerciali né utilizzare le informazioni personali raccolte nell'ambito dei servizi principali per scopi pubblicitari.	ADEGUATO
Chi può vedere i dati acquisiti ?	Le informazioni raccolte non vengono condivise senza uno specifico consenso con nessuno al di fuori di Google e non in circostanze limitate:	ADEGUATO

	Con gli amministratori interni alla scuola di G Suite for Education. Che hanno accesso alle informazioni archiviate negli account Google degli utenti di quella scuola o dominio. Per lavorazioni esterne. Anche Google talvolta fornisce informazioni personali a suoi affiliati o ad altre aziende o persone fidate affinché le elaborino per in nome e per conto di Google, sulla base di istruzioni e in conformità con l'informativa sulla privacy. Per motivi legali. Le informazioni personali possono essere condivise con terzi qualora ciò fosse necessario per soddisfare norme giuridiche o procedimenti legali o richiesta governativa applicabile, o per applicare i termini di servizio (indagini su potenziali violazioni), o per rilevare, prevenire o affrontare frodi, problemi di sicurezza o tecnici, o ancora proteggere da danni ai diritti, alla proprietà o alla sicurezza di Google, degli utenti o del pubblico come richiesto o consentito dalla legge. I genitori degli utenti di G Suite for Education nelle scuole primarie e secondarie possono accedere alle informazioni personali dei propri figli o richiederne l'eliminazione tramite l'amministratore della scuola. Se un genitore desidera interrompere qualsiasi ulteriore raccolta o utilizzo delle informazioni del proprio figlio, può richiedere che l'amministratore utilizzi i controlli del servizio a sua disposizione per limitare l'accesso dell'allievo a funzioni o servizi o eliminare completamente l'account.	
Sono adottate procedure di identificazione ed autenticazione degli utenti ?	Sì. Sono disponibili sistemi di autenticazione basati su password complesse e anche su password a due fattori	ADEGUATO
Sono presenti robusti processi di assegnazione agli utenti di credenziali ?	Sì. La creazione delle utenze viene eseguita dall'Istituto ad opera del soggetto interno autorizzato dalla scuola all'amministrazione della piattaforma.	ADEGUATO
Le password assegnate sono protette da una "password policies" adeguata ?	Sì, Il sistema permette di imporre che le password siano complesse (almeno 8 caratteri e composte sia da caratteri, minuscoli e maiuscoli, che da numeri) inoltre è possibile imporre una scadenza temporale alla validità della password. Tale scadenza nonché l'impostazione dell'obbligo di utilizzare password complesse è demandato all'attività del soggetto interno autorizzato dalla scuola all'amministrazione della piattaforma.	ADEGUATO
Sono definiti differenti profili di autorizzazione da attribuire ai soggetti autorizzati in modo da garantire un accesso selettivo ai dati ?	Sì, All'atto della creazione delle utenze ad opera del soggetto interno autorizzato dalla scuola all'amministrazione della piattaforma, lo stesso si preoccupa di definire delle policies di accesso esclusivo ai dati di sua pertinenza. I docenti possono accedere esclusivamente ai dati relativi agli allievi delle loro classi, gli allievi possono interagire esclusivamente con i loro compagni di classe.	ADEGUATO
I canali di trasmissione utilizzati sono sicuri sotto il profilo tecnico ?	E' in uso il protocollo TLS (Transport Layer Security) che consente di criptare e recapitare i messaggi di posta in modo sicuro, sia per il traffico in entrata che per quello in uscita, consentendo così di prevenire l'intercettazione dei messaggi durante il passaggio fra server di posta. Il rapporto Crittografia mostra il numero di messaggi criptati mediante TLS nel dominio. Google si avvale di diverse misure di sicurezza volte a garantire l'autenticità, l'integrità e la privacy dei dati in transito. Google crittografa e autentica tutti i dati in transito su uno o più livelli di rete quando i dati si spostano all'esterno dei confini fisici non controllati da Google o per conto di Google. I dati in transito all'interno di un confine fisico controllato da Google o per conto di Google sono generalmente autenticati, ma non necessariamente crittografati. A seconda della connessione effettuata, Google applica le misure di protezione predefinite ai dati in transito. Ad esempio, proteggiamo le comunicazioni tra l'utente e Google Front End (GFE) utilizzando TLS. I clienti di Google Cloud con requisiti aggiuntivi per la crittografia dei dati trasmessi su WAN possono scegliere di implementare ulteriori misure di protezione per i dati trasferiti da un utente a un'applicazione o da una macchina virtuale all'altra. Queste misure di protezione comprendono tunnel IPsec, S/MIME di Gmail, certificati SSL gestiti e Istio. Google collabora attivamente con il settore per contribuire a mettere la crittografia dei dati in transito a disposizione di tutti, ovunque. Abbiamo diversi progetti open source che incoraggiano l'uso della crittografia dei dati in transito e la sicurezza dei dati su Internet in generale, tra cui Certificate Transparency, le API di Chrome e SMTP sicuro.	ADEGUATO
Sono adottate soluzioni atte a garantire la disponibilità dei dati ?	G Suite presenta solo funzionalità limitate per il ripristino dei dati di G Suite perduti, distrutti o danneggiati e non dispone né delle funzionalità né dell'affidabilità delle soluzioni di backup con le quali molte attività proteggono le proprie applicazioni critiche. E' da dire tuttavia che i dati custoditi su G Suite sono da intendersi come dati principalmente didattici, pertanto pur trattandosi di una voce in cui la piattaforma non eccelle, la protezione garantita può dirsi adeguata se rapportata al tipo di dato trattato.	ADEGUATO
Sono adottati sistemi di protezione perimetrale ?	L'Istituto dispone di un firewall posto a monte della rete informatica che garantisce un adeguato livello di protezione perimetrale.	ADEGUATO

Sono adottati sistemi di protezione antivirus e antimalware ?	L'Istituto dispone di un software antivirus aggiornato che garantisce un adeguato livello di protezione rispetto alla distruzione e perdita dei dati.	ADEGUATO
I software di base vengono costantemente aggiornati ?	L'Istituto dispone di un programma di assistenza tecnica informatica che comprende anche l'aggiornamento dei sistemi operativi.	ADEGUATO
Degli accessi e delle operazioni compiute viene tenuta traccia registrando i file di log ?	E' in uso un sistema di registrazione e back up dei file di log riferiti alle utenze amministrative implementato dall'Amministratore di Sistema. I file di log di G Suite sono a disposizione del soggetto interno autorizzato dalla scuola all'amministrazione della piattaforma.	ADEGUATO
Sono definite le istruzioni da fornire ai soggetti autorizzati al trattamento ?	La Direzione Scolastica prevede la formazione di tutti gli autorizzati al trattamento dei dati.	ADEGUATO
Sono attuate misure di formazione e sensibilizzazione degli utenti ?	La Direzione Scolastica prevede l'informazione di tutti gli utilizzatori anche mediante la condivisione di un regolamento generale destinato agli allievi ed al personale utilizzatore della piattaforma.	ADEGUATO
E' stato necessario eseguire la DPIA ?	Come evidenziato nelle righe precedenti, l'esecuzione della D.P.I.A. non deve intendersi obbligatoria in quanto il trattamento in esame non appare ad elevato rischio e le misure di sicurezza attuate appaiono adeguate, tuttavia è stata volontà del Titolare del trattamento, consigliato in questa direzione dal D.P.O. eseguire comunque tale analisi approfondita. In conseguenza dell'analisi le misure di sicurezza definite dalla piattaforma Google Suite for Education appaiono ADEGUATE. Si rammenta che le stesse devono essere mantenute tali anche ad opera dell'Istituto Scolastico mediante l'adozione ed il mantenimento delle precauzioni specifiche di pertinenza del Titolare del trattamento che agisce per mezzo del soggetto interno autorizzato dalla scuola all'amministrazione della piattaforma che è stato formalmente individuato.	ADEGUATO