Istituto Comprensivo "Ferraris" di Vercelli

Ministero dell'Istruzione, dell'Università e della Ricerca. Ufficio Scolastico Regionale per il Piemonte.

Scuola Statale Infanzia – Primaria – Secondaria 1° grado
Piazza Cesare Battisti, 6 - 13100 VERCELLI
Tel. 0161/257999 - Fax 0161/501543 C.F.94023410023 - Cod. VCIC810005

PEO: vcic810005@istruzione.it PEC: vcic810005@pec.istruzione.it URL: www.icferraris.gov.it

PUA (Politica d'Uso Accettabile e Sicura della rete)

dell'I.C. Ferraris di Vercelli

Questa versione della PUA è stata creata da una Commissione, incaricata dal Dirigente Scolastico, sottoposta all'approvazione del Collegio dei Docenti e del Consiglio di Istituto.

La PUA fa parte delle strategie di uso consapevole delle TIC, si basa su linee guida delle politiche nazionali ed è strettamente connesso ad altri documenti predisposti dalla scuola:

- **ptof**
- **regolamento di Istituto**
- **e-policy**
- **informativa su GSuite for Education**
- **patto di corresponsabilità**

La suddetta documentazione è soggetta a revisione su base annuale.

Contenuti

1. I vantaggi di Internet a scuola

Il curricolo scolastico prevede che gli studenti imparino a trovare materiale, recuperare documenti e scambiare informazioni utilizzando le TIC. Internet offre sia agli studenti sia agli insegnanti una vasta scelta di risorse diverse e opportunità di scambi culturali con gli studenti di altri paesi. Inoltre, su internet si possono recuperare risorse per il tempo libero, le attività scolastiche e sociali.

La scuola propone agli studenti e agli insegnanti di utilizzare internet per promuovere l'eccellenza in ambito didattico attraverso la condivisione delle risorse, l'innovazione e la comunicazione. Per gli studenti e per gli insegnanti l'accesso ad internet è un privilegio e un diritto. Poiché esiste la possibilità che gli studenti trovino materiale inadeguato e illegale su internet, la scuola ha cercato di prendere delle precauzioni limitando l'accesso ad internet.

Gli insegnanti hanno la responsabilità di guidare gli studenti nelle attività on-line, di stabilire obiettivi chiari nell'uso di internet e insegnando un uso di internet accettabile e responsabile. L'obiettivo principale resta quello di arricchire ed ampliare le attività didattiche, secondo quanto prevede il curricolo scolastico, l'età e la maturità degli studenti.

2. Accertamento dei rischi e valutazione dei contenuti di internet

La scuola si fa carico di tutte le precauzioni necessarie per garantire agli studenti l'accesso a materiale appropriato, anche se non è possibile evitare che gli studenti trovino materiale indesiderato navigando su un computer della scuola. La scuola non può farsi carico della responsabilità per il materiale trovato su internet o per eventuali conseguenze causate dall'accesso ad internet. **Pertanto, a tutela degli alunni, la scuola richiede la collaborazione attiva e continua della famiglia e un controllo costante e puntuale dei dispositivi dei ragazzi.**

Gli studenti imparano ad utilizzare i metodi di ricerca su internet, l'uso dei motori di ricerca, comprese le modalità avanzate. Ricevere e inviare informazioni o messaggi e-mail prevede una buona abilità di gestione delle informazioni e della comunicazione. Le abilità di gestione delle informazioni includono:

1. la capacità di valutare e verificare l'attendibilità e l'aggiornamento delle fonti
2. l'utilizzo di fonti comparate
3. rispetto dei diritti d'autore e dei diritti di proprietà intellettuale.

Gli studenti devono essere pienamente coscienti dei rischi a cui si espongono quando sono in rete. Devono essere educati a riconoscere ed a evitare gli aspetti negativi di internet come la pornografia, la violenza, il razzismo e lo sfruttamento dei minori.

Agli studenti non dovrebbe essere sottoposto materiale di questo tipo e se ne venissero a contatto dovrebbero sempre riferire l'indirizzo internet (URL) all'insegnante o al coordinatore tecnico delle TIC.

È inoltre necessario fare un breve, ma importante riferimento ai rischi legati all'utilizzo degli archivi informatici:

1. utilizzo della rete da parte di personale non autorizzato ad accedere ai dati.
2. intrusioni da parte di studenti
3. accesso ai dati da parte di persone estranee all'amministrazione attraverso gli eventuali punti di ingresso/uscita verso internet.
4. intrusioni nel sistema da parte di hacker/cracker
5. scaricamento virus e/o trojan per mezzo di posta elettronica e/o operazioni di download eseguite tramite il browser.

3. Strategie della scuola per garantire la sicurezza dell'utilizzo delle TIC

La scuola per garantire la sicurezza nell'utilizzo delle TIC provvede anzitutto alla formazione constante di docenti e studenti. Inoltre utilizza una serie di accorgimenti.

1. Utilizzo di firewall per impedire l'accesso dall'esterno ai computer della scuola.
2. Uso, anche nella didattica, di sistemi operativi che permettono una efficace gestione della multiutenza.
3. L'utilizzo dei laboratori di informatica è regolamentato da un apposito orario settimanale e comunque gli alunni possono accedere solo se accompagnati da docenti, responsabili dell'utilizzo corretto dei dispositivi e della tempestiva segnalazione di guasti o danni. Ogni laboratorio è fornito di registro orario che deve essere debitamente compilato e firmato. (Si veda il documento relativo all'utilizzo dei laboratori allegato
4. L'accesso ai PC della scuola da parte degli studenti avviene sempre sotto sorveglianza dei docenti
5. Il sistema informatico delle TIC della scuola viene regolarmente controllato, per prevenire ed eventualmente rimediare a possibili disfunzioni dell'hardware e/o del software, dagli amministratori della rete, assistenti tecnici e/o professori.
6. La scuola controlla (per tramite dei docenti autorizzati e tecnici informaci esterni) regolarmente i file utilizzati, i file temporanei e i siti visitati.
7. È vietato inserire file sul server o scaricare software non autorizzati da internet.
8. Il sistema informatico della scuola è provvisto di un software antivirus aggiornato automaticamente o periodicamente dagli assistenti tecnici responsabili di laboratorio.
9. Per utilizzare chiavette USB o CD-ROM personali è necessario chiedere un permesso e sottoporli al controllo antivirus.
10. In generale il software utilizzabile è solamente quello autorizzato dalla scuola, regolarmente licenziato e/o open source.
11. Il filtro dei contenuti avviene attraverso un firewall che fa da server proxy configurabile internamente.

4. Norme e linee guida

Tutti gli utenti connessi ad internet devono rispettare:

1. la legislazione vigente applicata anche alla comunicazione su internet;
2. la **netiquette** (etica e norme di buon uso dei servizi di rete)**. Il sistema di accesso ad internet della scuola prevede l'uso di un filtro** per impedire l'accesso a contenuti non compatibili con la politica educativa della scuola (sesso, violenza, droghe, comportamenti criminali, occultismo, appuntamenti ed incontri, giochi d'azzardo, ecc.). Per maggior dettaglio si veda il §11.d.

L'amministratore della rete locale, il Dirigente scolastico o un suo delegato, effettua**, a scopo statistico funzionale,** il **monitoraggio dei siti visitati dagli utenti della rete scolastica e l'effettivo traffico dati. Dopo un certo numero di violazioni delle regole stabilite dalla politica scolastica, la scuola ha il diritto di eliminare l'accesso dell'utente a internet per un certo periodo di tempo o in modo permanente.**

La scuola riferisce alle autorità competenti se è stato trovato materiale illegale.

4.a Fornitore di servizi internet

1. Gli studenti devono utilizzare durante l'orario scolastico solo fornitori di servizi e-mail approvati dalla Scuola, previa autorizzazione del docente.
2. Gli studenti dovrebbero riferire agli insegnanti se ricevono e-mail offensive.
3. Gli studenti non devono rivelare dettagli o informazioni personali loro o di altre persone di loro conoscenza, come indirizzi, numeri di telefono...
4. L'invio e la ricezione di allegati è soggetto al permesso dell'insegnante.

4.b Mailing list moderate, gruppi di discussione e chat room

La scuola può utilizzare una lista di indirizzi di utenti selezionati per distribuire del materiale. L'insegnante è il moderatore degli altri mezzi di collaborazione, dei gruppi di discussione e delle chat room se sono utilizzati a scuola (Google Classroom, Registro elettronico).

1. Agli studenti non è consentito l'accesso alle chat room pubbliche o non moderate.
2. Sono permessi solo chat a scopi didattici e comunque sempre con la supervisione (**NON** la partecipazione diretta) dell'insegnante per garantire la sicurezza (ad esempio gruppo Whatsapp di classe)
3. Solo i gruppi di discussione che hanno obiettivi e contenuti didattici sono disponibili per gli studenti.

5. Gestione del sito web e della pagina Facebook della scuola.

5.a Sito WEB (www.icferraris.edu.it)

Il sito WEB della scuola è gestito dal Dirigente e dai suoi delegati che garantiscono che il contenuto sul sito sia accurato e appropriato. Il sito assolverà alle linee guida sulle pubblicazioni della scuola.

La scuola detiene i diritti d'autore dei documenti che si trovano sul sito; quelli distribuiti sotto licenza Creative Commons possono essere riutilizzati liberamente dichiarandone la provenienza.

Le informazioni pubblicate sul sito della scuola relative alle persone da contattare devono includere solo l'indirizzo della scuola, l'indirizzo di posta elettronica e il telefono della scuola, ma non informazioni relative agli indirizzi privati del personale della scuola o altre informazioni del genere. La scuola non pubblicherà materiale prodotto dagli studenti minorenni senza il permesso dei loro genitori; inoltre, le fotografie degli studenti non verranno pubblicate senza il consenso scritto del genitore o tutore se minorenne.

Dall'A.S. 2019-2020 le liberatorie sono pubblicate e raccolte all'interno del diario scolastico fornito gratuitamente dalla scuola e unico strumento autorizzato per lo scopo.

5.b Pagina Facebook (@IstitutoComprensivoFerrarisVercelli)

La pagina Facebook di Istituto è gestita dall'animatore digitale sotto la supervisione del Dirigente scolastico.

Il materiale pubblicato ha lo scopo di mettere in luce progetti, attività, riconoscimenti di tutti i plessi della scuola. Previa liberatoria da parte delle famiglie, potranno essere pubblicate immagini degli alunni, privilegiando le visioni di insieme rispetto al primo piano di singoli alunni.

6. Utilizzo dispositivi

6.a Utilizzo di dispositivi della scuola.

La scuola fornisce a docenti, personale ATA e studenti l'uso di apparecchiature informatiche di vario tipo. Gli studenti possono utilizzarle solo sotto la supervisione dei docenti.

Per un'indicazione dettagliata di comportamenti leciti e vietati si veda §8. Qui si ricordano alcuni aspetti fondamentali.

1. Su dispositivi comuni dove i dati non sono protetti da password **non si possono archiviare informazioni sensibili**

2. Quando ci si connette a un dispositivo condiviso non si devono salvare password di accesso e al termine dell'utilizzo bisogna sempre ricordarsi di **effettuare il logout** da aree riservate (soprattutto registro elettronico e mail personale)

3. Sulla LIM è preferibile non accedere al **registro di classe**. Qualora sia necessario accedere ricordarsi di effettuare il Logout al termine dell'utilizzo e in ogni caso **NON** è consentito aprire pagine del registro di fronte alla classe con dati personali degli studenti.

4. Nell'utilizzo di dispositivi comuni si presterà massima cura a non danneggiarli nelle componenti hardware e software. I docenti vigileranno sul comportamento degli alunni in quanto i dispositivi della scuola possono essere usati dagli studenti **SOLO sotto la supervisione dei docenti. NON è consentito autorizzare gli studenti a utilizzarli in autonomia.**

6.b Utilizzo di dispositivi privati

Nell'Istituto non è consentito agli **alunni** l'utilizzo di telefoni cellulari per scopi privati (se vengono portati a scuola, vanno tenuti spenti). In caso di urgenza per comunicazioni tra gli alunni e le famiglie, su autorizzazione dei docenti e sotto il diretto controllo dei collaboratori scolastici, gli alunni potranno comunicare con le famiglie tramite gli apparecchi telefonici della scuola, pertanto è indispensabile che le famiglie forniscano recapiti telefonici a cui possano essere facilmente reperibili.

Per quanto concerne l'utilizzo dei tablet o PC portatili (Attività BYOD – Bring your own device), potranno essere utilizzati solo se permessi dal docente, alla presenza del docente e per ragioni prettamente scolastiche.

Discorso a parte meritano le classi iPad, in cui l'utilizzo del dispositivo privato è parte integrante del percorso didattico scelto. Gli studenti avranno cura del proprio dispositivo che deve essere provvisto di un codice di blocco schermo in modo che non sia possibile ad altri accedere ai contenuti privati. Durante l'intervallo l'iPad deve rimanere in classe riposto con cura. In caso di uscita della classe, l'aula verrà chiusa a chiave dal personale per evitare danneggiamento colposo o intenzionale dei dispositivi, utilizzo non autorizzato e furti.

Durante le ore di lezione è consentito ai docenti e al personale l'uso di cellulari, PC portatili e tablet di loro proprietà a scopo lavorativo, didattico e ad integrazione dei dispositivi scolastici disponibili (Attività BYOD – Bring your own device). Il docente, con il proprio User Id, potrà collegare al wi-fi della scuola fino a un massimo di due dispositivi, tuttavia, per non sovraccaricare la linea è preferibile che ogni docente colleghi un solo dispositivo.

6.b Acquisizione disponibilità consenso famiglie utilizzo segnale wireless

L'intero Istituto è coperto da segnale wireless. All'atto dell'iscrizione dello studente all'Istituto i genitori/tutori accettano la E-Policy e il Patto di corresponsabilità, dando il consenso e la disponibilità affinché possa essere utilizzato il segnale wireless.

L'Istituto ha in programma un'azione di progressivo miglioramento e potenziamento della rete wi-fi, tale da rendere presto disponibile il servizio wi-fi a tutti gli studenti che potranno collegarsi attraverso dispositivi personali (BYOD). L'utilizzo dei dispositivi personali durante le ore di lezione sarà riferito a sola connotazione didattica e sotto il controllo del docente responsabile della lezione.

7. Informare sulla Politica d'Uso Accettabile (PUA) della scuola

7.a Informare gli studenti sulla PUA della scuola

Le regole di base relative all'accesso ad internet verranno comunicate e diffuse tramite **registro elettronico e sito** della scuola. Gli studenti saranno informati che l'utilizzo di internet è monitorato e verranno date loro delle istruzioni per un uso responsabile e sicuro di internet. Gli studenti e i loro genitori/tutori accettano i regolamenti al momento dell'iscrizione in particolare quanto definito in E-Policy e patto di Corresponsabilità

7.b Informare il personale scolastico della PUA

Sul sito della Scuola e nella Bacheca del registro sarà disponibile copia della Politica d'Uso Accettabile della scuola in modo che tutto il personale possa prenderne accurata visione ed essere consapevole che l'uso di internet verrà monitorato per garantire la sicurezza e il rispetto delle norme vigenti.

Gli insegnanti e tutto il personale d'Istituto accettano il Regolamento per l'utilizzo della rete.

In caso di dubbi legati alla legittimità di una certa istanza utilizzata in internet, l'insegnante dovrà contattare il Dirigente scolastico / il responsabile di rete per evitare malintesi. Gli insegnanti saranno provvisti di informazioni concernenti le problematiche sui diritti d'autore che vengono applicate alla scuola.

7.c Informare i genitori/tutori sulla PUA della scuola

Le famiglie e gli studenti potranno visionare la PUA, l'E-Policy e il patto di corresponsabilità sul sito della Scuola e sulla Bacheca del Registro elettronico. Sarà inoltre possibile trovare, in formato essenziale, tali documenti anche sul diario fornito agli studenti, dove le famiglie potranno sottoscriverli e firmare le liberatorie predisposte dalla scuola.

8) Regolamento per l'utilizzo della rete

8.a *Oggetto e ambito di applicazione*

Il presente regolamento disciplina le modalità di accesso e di uso della rete informatica e telematica dell'I.C. Ferraris e dei servizi che, tramite la stessa rete, è possibile ricevere o offrire.

8.b Principi generali – diritti e responsabilità

L'Istituto Comprensivo Ferraris promuove l'utilizzo della rete quale strumento utile sia nella gestione della scuola sia nella didattica. Consapevoli delle potenzialità offerte dagli strumenti informatici e telematici, gli utenti si impegnano ad agire con responsabilità e a non commettere abusi aderendo a un principio di autodisciplina.

Le attrezzature informatiche fornite (computer, LIM, tablet, altro hardware) vengono consegnate complete di quanto necessario per svolgere le proprie funzioni, pertanto è vietato modificarne la configurazione. Il software installato è quello richiesto dalle specifiche attività lavorative dell'operatore. È pertanto proibito installare qualsiasi programma non autorizzato da parte dell'utente o di altri operatori, escluso l'Amministratore di sistema o suo delegato.

Ogni utente è responsabile dei dati memorizzati nei dispositivi utilizzati.

8.c Abusi e attività vietate

Si intende con abuso qualsiasi violazione del presente regolamento e di altre norme civili, penali e amministrative che disciplinano le attività e i servizi svolti sulla rete e di condotta personale.

È vietato ogni tipo di abuso. In particolare **è proibito**:

1. Usare la rete in modo difforme da quanto previsto dalle leggi penali, civili e amministrative.

2. Usare la rete in modo difforme da quanto previsto dal presente regolamento.

3. Utilizzare la rete per scopi incompatibili con l'attività istituzionale dell'I.C. Ferraris.

4. Utilizzare credenziali di accesso a cui non si è autorizzati o accedere senza autorizzazione a risorse di rete interne o esterne.

5. Cedere a terzi codici personali di accesso al sistema e/o alla rete.

6. Violare la riservatezza di altri utenti o di terzi.

7. Agire deliberatamente con attività che influenzino negativamente la regolare operatività della rete e ne restringano l'utilizzabilità e le prestazioni per altri utenti.

8. Fare o permettere ad altri trasferimenti non autorizzati di informazioni (software, basi dati, ecc.).

9. Installare o eseguire deliberatamente o diffondere su qualunque computer e sulla rete, programmi destinati a danneggiare o sovraccaricare i sistemi o la rete (p. es. virus, cavalli di troia, worms, spamming della posta elettronica, programmi di file sharing ...).

10. Installare o eseguire deliberatamente programmi software non autorizzati e non compatibili con le attività istituzionali.

11. Cancellare, disinstallare, copiare o asportare deliberatamente programmi software per scopi personali.

12. Installare deliberatamente componenti hardware non compatibili con le attività istituzionali.

13. Rimuovere, danneggiare deliberatamente o asportare componenti hardware.

14. Utilizzare le risorse hardware e software e i servizi disponibili per scopi personali.

15. Utilizzare le caselle di posta elettronica di Istituto per scopi personali e/o non istituzionali. Accedere alla suddetta casella con le credenziali di autenticazione di altri utilizzatori. Inviare e ricevere materiale che violi le leggi.

16. Utilizzare l'accesso ad Internet per scopi personali.

17. (Per gli studenti) accedere ad Internet attraverso reti personali non autorizzate

18. Monitorare o utilizzare qualunque tipo di sistema informatico o elettronico per controllare le attività degli utenti, leggere copiare o cancellare files e software di altri utenti, senza averne l'autorizzazione esplicita.

19. Usare l'anonimato o servirsi di risorse che consentano di restare anonimi sulla rete.

20. Abbandonare il posto di lavoro lasciandolo incustodito o accessibile

21. Rivelare ad altri le proprie credenziali di accesso (alla rete wi-fi a G-Suite for Education) o permettere ad altri di utilizzarle; accedere con credenziali non proprie.

8.d Attività consentite

È consentito agli Amministratori di sistema:

1. Monitorare o utilizzare qualunque tipo di sistema informatico o elettronico per controllare il corretto utilizzo delle risorse di rete, dei client e degli applicativi, per copiare o rimuovere files e software, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori.

2. Creare, modificare, rimuovere o utilizzare qualunque credenziale di accesso, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori. L'Amministratore darà comunicazione dell'avvenuta modifica all'utente.

3. Rimuovere programmi software, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori.

4. Rimuovere componenti hardware, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori.

8.e Soggetti che possono avere accesso alla rete

Hanno diritto ad accedere alla rete di Istituto tutti i dipendenti, gli studenti per attività didattiche, le ditte fornitrici di software per motivi di manutenzione e limitatamente alle applicazioni di loro competenza, collaboratori esterni impegnati nelle attività istituzionali per il periodo di collaborazione. L'accesso alla rete è assicurato compatibilmente con le potenzialità delle attrezzature e della linea.

L'Amministratore di sistema può regolamentare l'accesso alla rete di determinate categorie di utenti, quando questo è richiesto da ragioni tecniche, amministrative o didattiche. Per consentire l'obiettivo di assicurare la sicurezza e il miglior funzionamento delle risorse disponibili l'Amministratore di Sistema può proporre al Titolare del trattamento l'adozione di appositi regolamenti di carattere operativo che gli utenti si impegnano ad osservare.

L'accesso agli applicativi è consentito agli utenti che, per motivi di servizio, ne

devono fare uso.

8.f Modalità di accesso alla rete e agli applicativi

L'utente che ottiene l'accesso alla rete e agli applicativi si impegna ad osservare il presente regolamento e le altre norme disciplinanti le attività e i servizi che si svolgono via rete e si impegna a non commettere abusi e a non violare i diritti degli altri utenti e di terzi.

L'utente che ottiene l'accesso alla rete e agli applicativi si assume la totale responsabilità delle attività svolte tramite la rete.

L'utente è tenuto a verificare l'aggiornamento periodico del software antivirus e a segnalare la necessità di manutenzione e/o aggiornamento.

Le credenziali personali sono segrete e NON devono essere comunicate ad altri. Vanno custodite con diligenza e riservatezza, in quanto stabiliscono un rapporto biunivoco, che permette di responsabilizzare l'incaricato stesso. Le password devono essere sufficientemente sicure.

L'utente deve sostituire la parola chiave, nel caso ne accertasse la perdita o ne verificasse una rivelazione.

8.g Sanzioni

In caso di abuso, a seconda della gravità del medesimo, e fatte salve ulteriori conseguenze di natura penale, civile e amministrativa, possono essere comminate le sanzioni disciplinari previste dalla normativa vigente in materia.

9)- Utilizzo del proxy

L'utilizzo del proxy riguarda le misure procedurali relative all'identificazione e autenticazione degli utenti, le regole di utilizzo delle risorse hardware e software, le norme comportamentali e le responsabilità di ciascuno. Rientrano in questo aspetto le norme di comportamento interno per limitare l'uso privato di e-mail o Internet, in quanto i controlli sono possibili solo a determinate condizioni e con l'accordo delle Rappresentanze Sindacali Unitarie. Il Regolamento Europeo per la protezione dei dati - GDPR 25 MAGGIO 2018 - non contrasta con quanto dettato dall'art. 4 dello Statuto dei Lavoratori, ovvero il divieto di utilizzo da parte del datore di lavoro di apparecchiature atte al controllo a distanza dell'attività del lavoratore, salvo che esigenze organizzative, produttive o di sicurezza non abbiano determinato, previo accordo con le rappresentanze sindacali, la lecita introduzione in azienda".

D'altro canto la consultazione di siti web da parte del lavoratore o l'utilizzo di posta elettronica durante il normale orario di lavoro non è consentita quando tale attività non sia pertinente con le mansioni affidate, come l'art. 1024 del codice civile prevede nel principio generale di diligenza del lavoratore. Per trovare un punto di equilibrio tra i diritti del lavoratore e dell'istituto è opportuno introdurre una policy trasparente e codificata con l'apporto dei lavoratori, dando anche la possibilità al datore di lavoro di prevedere meccanismi sanzionatori, sempreché la policy sia resa accessibile a tutti i lavoratori, come previsto dall'art. 7 dello Statuto dei Lavoratori.

Per quanto riguarda le politiche di sicurezza si può fare riferimento alle responsabilità civili e penali per i danni cagionati con il trattamento dei dati personali.

A titolo di esempio si possono elencare:

- la responsabilità civile disciplinata dall'art. 2050 del Codice Civile "chi cagiona danno ad altri per effetto del trattamento dei dati personali è tenuto a risarcire il danno, a meno che non provi di aver adottato tutte le misure idonee per evitarlo"
- la sanzione penale colpisce chi, essendovi tenuto in base alle norme vigenti, omette di adottare le misure di sicurezza

Le informazioni e le attività eseguite sulla rete informatica e telematica di Istituto relative agli utilizzatori sono registrate; è possibile tracciare la navigazione, i tracciati vengono salvati in modalità cifrata e potranno essere accessibili solo su richiesta del Dirigente Scolastico.

10- Misure di sicurezza, incident response, ripristino

Le misure di sicurezza di carattere elettronico/informatico sono quelle in grado di segnalare gli accessi agli elaboratori, agli applicativi, ai dati e alla rete, di gestire le copie di salvataggio dei dati e degli applicativi, di assicurare l'integrità dei dati, di proteggere gli elaboratori da programmi volutamente o involontariamente ritenuti dannosi.

Le misure adottate sono:

1. presenza di gruppi di continuità elettrica per il server
2. archiviazione e backup di dati
3. installazione di un sistema antivirus su tutte le postazioni di lavoro.
4. definizione delle regole di comportamento per minimizzare i rischi da virus, di seguito riportate;
5. installazione di un firewall con hardware dedicato per proteggere la rete dagli accessi indesiderati attraverso internet*;*
6. definizione delle regole per la gestione delle credenziali di accesso;
7. definizione delle regole per la gestione di strumenti elettronici/informatici, di seguito riportate;
8. divieto di memorizzare dati personali, sensibili, giudiziari sulle postazioni di lavoro non autorizzate a tale scopo.

10.a Regole per la gestione delle password

Tutti gli incaricati del trattamento dei dati personali accedono al sistema informatico per mezzo di un codice identificativo personale (user-id) e password personale. User-id e password iniziali sono assegnati dall'Amministratore di sistema o da un suo delegato, sono strettamente personali e non possono essere riassegnate ad altri utenti.

Le password di amministratore di tutti i PC che lo prevedono sono assegnate dall'Amministratore di sistema o da suo delegato. In caso di necessità l'Amministratore di sistema è autorizzato a intervenire sui personal computer.

Gli account del personale che per scadenze contrattuali, trasferimenti, pensionamenti o altri motivi non saranno più dipendenti di questa istituzione scolastica, verranno bloccati.

In caso di manutenzione straordinaria possono essere comunicate, qualora

necessario, dall'Amministratore di sistema al tecnico/sistemista addetto alla manutenzione le credenziali di autenticazione di servizio. Al termine delle operazioni di manutenzione l'Amministratore di sistema deve disabilitare le credenziali di autenticazione.

Le regole di seguito elencate sono vincolanti per tutti i posti lavoro tramite i quali si può accedere alla rete e alle banche dati contenenti dati personali e/o sensibili.

Le password assegnate inizialmente e quelle di default dei sistemi operativi, prodotti software, ecc. sono da cambiare dopo l'installazione e al primo utilizzo.

10.b Regole per la gestione degli strumenti elettronici/informatici

Per gli elaboratori che ospitano archivi (o hanno accesso tramite la rete) con dati personali sono adottate le seguenti misure:

1. l'accesso agli incaricati ed agli addetti alla manutenzione è possibile solo in seguito ad autorizzazione scritta;

2. gli hard disk non sono condivisi in rete se non temporaneamente per operazioni di copia;

3. tutte le operazioni di manutenzione avvengono con la supervisione dell'incaricato del trattamento dati o di un suo delegato;

4. le copie di backup sono conservate in un luogo di non facile accesso a chiunque, chiuso a chiave con accesso consentito al solo personale autorizzato.

5. divieto per gli utilizzatori di strumenti elettronici di lasciare incustodito, o accessibile, lo strumento elettronico stesso.

6. divieto di memorizzazione di archivi con dati sensibili di carattere personale dell'utente sulla propria postazione di lavoro non inerenti alla funzione svolta;

7. divieto di installazione di software di qualsiasi tipo sui personal computer che contengono archivi con dati sensibili senza apposita autorizzazione scritta da parte del responsabile del trattamento dati.

Il controllo dei documenti stampati è responsabilità degli incaricati al trattamento dati.

La stampa di documenti contenenti dati sensibili è effettuata su stampanti

poste in locali ad accesso controllato o presidiate dall'incaricato.

La manutenzione degli elaboratori, che può eventualmente prevedere il trasferimento fisico presso un laboratorio riparazioni, è autorizzata solo a condizione che il fornitore del servizio dichiari per iscritto di avere redatto il documento programmatico sulla sicurezza e di aver adottato le misure minime di sicurezza previste dal disciplinare.

10.c Regole di comportamento per minimizzare i rischi da virus

Per minimizzare il rischio da virus informatici, gli utilizzatori dei PC adottano le seguenti regole:

1. limitare lo scambio fra computer di supporti rimovibili (es. chiavette usb).

2. controllare (scansionare con un antivirus aggiornato) qualsiasi supporto prima di operare su uno qualsiasi dei file in esso contenuti;

3. evitare l'uso di programmi shareware e di pubblico dominio se non se ne conosce la provenienza, ovvero divieto di "scaricare", senza autorizzazione, dalla rete internet ogni sorta di file, eseguibile e non.

4. non aprire gli allegati di posta se non si è certi della loro provenienza, e in ogni caso analizzarli con un software antivirus. Usare prudenza anche se un messaggio proviene da un indirizzo conosciuto (alcuni virus prendono gli indirizzi dalle mailing list e della rubrica di un computer infettato per inviare nuovi messaggi "infetti");

5. non cliccare mai un link presente in un messaggio di posta elettronica da provenienza sconosciuta,(in quanto potrebbe essere falso e portare a un sito-truffa);

6. non utilizzare le chat personali, non autorizzate per la didattica;

7. Seguire scrupolosamente le istruzioni fornite dal sistema antivirus nel caso in cui tale sistema antivirus abbia scoperto tempestivamente il virus (in alcuni casi esso è in grado di risolvere il problema, in altri chiederà di eliminare o cancellare il file infetto);

8. avvisare l'Amministratore di sistema nel caso in cui il virus sia stato scoperto solo dopo aver subito svariati malfunzionamenti della rete o di qualche PC, ovvero in ritardo, (in questo caso è possibile che l'infezione abbia raggiunto parti vitali del sistema);

9. conservare i dischi di ripristino, se presenti, del proprio PC (creati con l'installazione del sistema operativo, o forniti direttamente dal costruttore del PC);

10. conservare le copie originali di tutti i programmi applicativi utilizzati e la copia di backup consentita per legge;

11. conservare la copia originale del sistema operativo e la copia di backup consentita per legge;

12. conservare i driver delle periferiche (stampanti, schede di rete, monitor ecc. fornite dal costruttore).

Nel caso di sistemi danneggiati seriamente da virus, l'Amministratore procede a reinstallare il sistema operativo, i programmi applicativi ed i dati.

10.d Incident response e ripristino

Tutti gli incaricati del trattamento dei dati devono avvisare tempestivamente il responsabili della sicurezza informatica o l'amministratore di sistema o il responsabile del trattamento dei dati, nel caso in cui constatino le seguenti anomalie:

1. Discrepanze nell'uso degli user-id;
2. modifica e sparizione di dati;
3. cattive prestazioni del sistema (così come percepite dagli utenti);
4. irregolarità nell'andamento del traffico;
5. irregolarità nei tempi di utilizzo del sistema;
6. quote particolarmente elevate di tentativi di connessione falliti.

In caso di incidente sono considerate le seguenti priorità:

1. evitare danni diretti alle persone;
2. proteggere l'informazione sensibile o proprietaria;
3. evitare danni economici;
4. limitare i danni all'immagine dell'organizzazione.

Garantita l'incolumità fisica alle persone si procedere a:

1. isolare l'area contenente il sistema oggetto dell'incidente;
2. isolare il sistema compromesso dalla rete;
3. fotografare e spegnere correttamente il sistema oggetto dell'incidente. Una volta spento il sistema oggetto dell'incidente non deve più essere riacceso;

4. documentare tutte le operazioni.

Se l'incidente è dovuto ad imperizia del personale o ad eventi accidentali, ovvero quando non vi è frode, danno, abuso e non è configurabile nessun tipo di reato, il ripristino può essere effettuato, a cura dell'Amministratore di sistema, direttamente sugli hard disk originali a partire dalle ultime copie di backup ritenute valide.

Altrimenti il Titolare del trattamento, il Responsabile del trattamento e l'Amministratore di sistema coinvolgeranno esperti e/o autorità competenti.

11- Regole di utilizzo della mail istituzionale e G-Suite for Education

I docenti di tutti i plessi e gli studenti della scuola Secondaria ricevono una mail istituzionale (nome.cognome@vergaferraris.net) con cui possono accedere ai servizi di **G-Suite for Education.**

Per ricevere tali credenziali il personale e le famiglie dovranno leggere e sottoscrivere il regolamento, il patto di responsabilità e le liberatorie previste dalla scuola impegnandosi ad utilizzare tale servizio per scopi didattici e nel rispetto delle norme condivise.

La mail istituzionale fornita agli studenti permette di scrivere e ricevere mail o condividere materiale solo all'interno del dominio (@vergaferraris.net), pertanto ai fini esclusivamente didattici e sotto la supervisione del docente è consentito l'utilizzo di un indirizzo di posta elettronica personale (predisposto dalla famiglia per l'alunno). Tale eventualità può nascere da esigenze didattiche di utilizzo di piattaforme online, libri digitali o applicazioni che richiedono la registrazione di un account personale.

Le applicazioni utilizzate per la scuola saranno gratuite e accuratamente selezionate e testate dal docente prima di essere presentate agli studenti.

L'utilizzo della posta elettronica personale dovrà osservare le stesse regole di utilizzo presenti in questo documento per gli account di Istituto.

L'istituto non si ritiene responsabile di un eventuale utilizzo improprio dell'indirizzo e-mail personale da parte dello studente.

11.a Durata del rapporto

Il rapporto per l'uso della mail istituzionale coincide con la durata di permanenza nell'Istituto.

L'account verrà sospeso quando lo studente non frequenterà più l'I.C. Ferraris e il docente (o altro dipendente della scuola) non lavorerà più nell'Istituto. Sarà cura di docenti e studenti salvare eventuali dati personali su altri servizi cloud personali o su supporti esterni.

Per provvedere al backup dei dati verranno concessi 60 giorni di tempo, al termine dei quali l'account istituzionale verrà cancellato.

11.b Obblighi di docenti e studenti

I Docenti si impegnano a:

1. a conservare le credenziali personali e a non consentirne l'uso ad altre persone

2. a non consentire ad altri, a nessun titolo, l'utilizzo della propria mail Istituzionale o delle applicazioni ad esso collegate;
3. a utilizzare l'account Istituzionale a scopo didattico o comunque connesso ad attività collegate alle esigenze della scuola.
4. a formare gli studenti insegnando non solo l'utilizzo tecnico delle applicazioni e della tecnologia, ma soprattutto un uso consapevole e rispettoso delle norme
5. a non diffondere eventuali informazioni riservate di cui venissero a conoscenza, relative all'attività delle altre persone che utilizzano il servizio

Gli studenti si impegnano:

1. a conservare le credenziali personali e a non consentirne l'uso ad altre persone;
2. a comunicare immediatamente ai propri docenti l'impossibilità ad accedere al proprio account o il sospetto che altri possano accedervi;
3. a non consentire ad altri, a nessun titolo, l'utilizzo della propria mail Istituzionale o delle applicazioni ad esso collegate;
4. a utilizzare esclusivamente l'indirizzo istituzionale per le comunicazioni con docenti e compagni di classe e solo a scopi didattici
5. a non diffondere eventuali informazioni riservate di cui venissero a conoscenza, relative all'attività delle altre persone che utilizzano il servizio;
6. ad osservare il presente regolamento, pena la sospensione da parte dell'Istituto dell'account personale dello studente;
7. ad utilizzare i servizi offerti solo ad uso esclusivo per le attività didattiche della scuola. Lo studente è consapevole di tutti i dati da lui inoltrati, creati e gestiti attraverso la piattaforma.

Le famiglie si impegnano a:

Vigilare sull'uso delle tecnologie da parte dei propri figli con particolare attenzione ai tempi, alle modalità e agli atteggiamenti conseguenti, ricordando che la famiglia si deve assumere la responsabilità dei dati condivisi dallo studenti e del suo comportamento on-line.

11.c. Limiti di Responsabilità

L'Istituto non si ritiene responsabile di eventuali danni arrecati allo studente a causa di guasti e/o malfunzionamenti del servizio e si impegna affinché la piattaforma Google funzioni nel migliore dei modi. (Si veda contratto siglato con Google)

L'Istituto non si ritiene responsabile di usi impropri da parte dei singoli degli strumenti forniti.

11.d Netiquette per lo studente

Di seguito sono elencate le regole di comportamento che ogni studente deve seguire affinché il servizio possa funzionare nel miglior modo possibile, tenendo presente che cortesia ed educazione, che regolano i rapporti comuni tra le persone, valgono anche in questo contesto.

Se si utilizza un dispositivo condiviso (quali i computer dei laboratori informatici o tablet forniti dalla scuola) si avrà cura di:

1. rispettare e utilizzare con cura i dispositivi accertandosi di accenderli e spegnerli in modo corretto
2. prestare massima attenzione a non danneggiarli nelle componenti di hardware e software
3. controllare di aver disconnesso il proprio account al termine dell'utilizzo;

Da dispositivi condivisi o privati lo studente si impegna a:

1. inviare (tramite mail o Google Classroom) messaggi inerenti alle attività didattiche specificando (per quanto riguarda la mail) sempre chiaramente l'oggetto in modo tale che il destinatario possa immediatamente individuarne l'argomento
2. non inviare lettere o comunicazioni a catena (es. catena di S. Antonio o altri sistemi di carattere "piramidale") che causano un inutile aumento del traffico in rete;
3. non utilizzare le piattaforme in modo da danneggiare, screditare, molestare o insultare altre persone;
4. non creare e non trasmettere immagini, dati o materiali osceni, indecenti, offensivi o comunque non autorizzati e/o di proprietà altrui.
5. non creare e non trasmettere materiali commerciali o pubblicitari se non espressamente richiesto;
6. rispettare gli altri utilizzando un linguaggio adeguato, educato e gentile
7. rispettare e non danneggiare il lavoro altrui, soprattutto quando si lavora su file condivisi;
8. non violare la riservatezza degli altri e il diritto di autore.
9. non divulgare i link delle video lezioni
10. non registrare le video lezioni nel rispetto della privacy altrui

11. sarebbe consigliabile durante le video lezioni tenere le webcam accese e i microfoni spenti, rispettando i turni di parola

L’infrazione alle regole nell’uso delle piattaforme informatiche comporta la sospensione dell'account istituzionale, della connessione al wi-fi della scuola e dell'utilizzo dei dispositivi personali o della scuola in orario scolastico. La sospensione dal servizio informatico sarà di durata proporzionale alla gravità dell'infrazione e potrà essere accompagnata a sanzioni disciplinari.

← 12) DaD: Didattica a Distanza

IL DPCM dell'8 marzo 2020 e la seguente nota ministeriale n. 279 hanno stabilito la necessità di attivare la **D**idattica **a D**istanza (**DaD**) per tutelare il diritto all'istruzione garantito dalla nostra Costituzione.

La registrazione della scuola alla G-Suite for Education e il registro elettronico ci hanno permesso di essere immediatamente operativi. Ovviamente le età molto diverse dei nostri utenti hanno richiesto una diversa strutturazione della DaD per infanzia, primaria e secondaria di I grado.

Sono inoltre state istituite una serie di mail help specifiche per i plessi in modo da guidare le famiglie nell'attività di DaD e nel recupero di credenziali.

La Scuola dell'Infanzia si è mossa fornendo alle famiglie spunti per attività domestiche, incentivando la creatività dei bambini e mantenendo un contatto con gli insegnanti. L'utilizzo di mail e gruppi whatsapp ha permesso la comunicazione con le famiglie

La Scuola Primaria ha gestito una DaD prevalentemente in modalità asincrona con consegna di attività e spiegazione (in forma scritta o videoregistrata) tramite registro elettronico e restituzione degli elaborati degli alunni attraverso mail istituzionale.

Si sono inoltre sperimentate video lezioni tramite l'utilizzo di Google Hangouts Meet, con l'intera classe o in piccoli gruppi a seconda della necessità e dell'età dell'utenza.

La Scuola Secondaria di I grado ha organizzato una DaD sia in modalità asincrona sia in modalità sincrona.

Modalità Asincrona

Per lo scambio di materiale e attività la scuola si è avvalsa di:

Registro elettronico: la sezione Didattica per trasmettere materiale multimediale e l'agenda per l'organizzazione delle attività.

Google Classroom: attraverso l'applicazione compresa nelle Google Apps for Education è stato possibile organizzare classi e corsi virtuali, in cui consegnare e ricevere materiale, comunicare con i ragazzi, assegnare e correggere compiti e verifiche.

Mail istituzionale: di cui sono provvisti non solo tutti i docenti, ma anche tutti gli studenti.

Modalità sincrona

Google Hangouts Meet: l'applicazione di Google ci ha permesso di continuare a svolgere quotidianamente lezione in video conferenza con le intere classi.

Si è previsto un orario curricolare mattutino di 15 moduli settimanali da 45' ciascuno in orario compreso tra le 9:30 e le 11:45. A questi 15 moduli si affiancano moduli aggiuntivi pomeridiani di recupero, potenziamento, sostegno e attività extracurricolari, cercando comunque di non costringere gli studenti a una permanenza troppo prolungata di fronte allo schermo e garantendo una distribuzione equilibrata delle attività.

In questo modo si è cercato di favorire l'inclusione, garantire un contatto diretto tra docenti e alunni e aiutare alunni e famiglie in difficoltà a non essere penalizzati nel percorso formativo.

Compatibilmente alle risorse fornite dal Ministero, si è cercato di fornire in comodato d'uso tramite bando tablet alle famiglie per superare il digital divide.

Tutte le applicazioni utilizzate sono gratuite e fruibili anche da smartphone e tablet.

Meet ha permesso inoltre di svolgere regolarmente tutte le attività collegiali: programmazione, consigli di classe, gruppi di lavoro, collegi, formazione garantendo al corpo docente la possibilità non solo di rimanere in contatto, ma anche di coordinarsi e procedere con coesione e coerenza didattica.

Nel periodo di emergenza Covid19 Google ha esteso le funzioni a pagamento di MEET a tutte le scuole (possibilità di registrare le video lezioni, estensione del numero massimo di partecipanti...).

Eventuali registrazioni saranno gestite dai docenti esclusivamente a scopo didattico (ad es. possibilità di registrare corsi di formazione per personale).

Per tutelare la privacy dei nostri alunni si è deciso di non registrare lezioni con la presenza dei ragazzi.

Nota: tra il materiale reperito sul web al fine di trarre documentazione e spunti per costituire il presente testo, la P.U.A. dell'I.I.S Alberto Castigliano di Asti (scuola all'avanguardia per l'integrazione delle risorse digitali nella didattica, nonché scuola di eccellenza nel campo informatico) è per noi stata un modello di riferimento, per completezza, puntualità e chiarezza.

ALLEGATO A

Informativa all'uso scolastico di GSuite for Education

Istituto Comprensivo Ferraris di Vercelli

a.s. 2020-2021

Gentili genitori e tutori,

vi informiamo che l'Istituto Comprensivo Ferraris di Vercelli utilizza il software G Suite for Education.

G Suite for Education consiste in una serie di strumenti gratuiti forniti da Google per aumentare la produttività didattica, tra cui Gmail, Calendar, Documenti Google, Classroom e altri ancora, che sono utilizzati da decine di milioni di studenti in tutto il mondo. Nella nostra scuola, gli studenti utilizzeranno i loro account G Suite per eseguire i compiti, comunicare con i loro insegnanti, accedere ai Chromebook scolastici e apprendere le competenze di cittadinanza digitale del XXI secolo.

L'informativa riportata di seguito risponde alle domande più comuni su come Google può o non può utilizzare le informazioni personali di vostro figlio, tra cui:

- Quali informazioni personali raccoglie Google?
- In che modo Google utilizza queste informazioni?
- Google divulga le informazioni personali di mio figlio?
- Google utilizza le informazioni personali degli utenti delle scuole primarie e secondarie per mostrare pubblicità mirata?
- Mio figlio può condividere informazioni con altre persone utilizzando l'account G Suite for Education?

Vi invitiamo a leggere con attenzione questo documento e comunicarci se avete dubbi e necessità di ulteriori chiarimenti.

Ricordiamo quanto sia stato indispensabile durante l'emergenza Covid-19 avere la possibilità di accesso ai servizi di Google per la Didattica a Distanza nell'ottica di poter garantire la formazione di bambini e ragazzi.

Inoltre, tutti gli alunni devono sviluppare le competenze digitali necessarie a poter gestire, in futuro, un'attività lavorativa anche attraverso lo smart working e, nell'immediato, un apprendimento completo e in linea con le richieste della società in cui viviamo.

Informativa su G Suite for Education per i genitori e i tutori

La presente informativa descrive le informazioni personali che forniamo a Google in relazione agli account e in che modo Google raccoglie, utilizza e divulga le informazioni personali degli studenti collegate a tali account.

Tramite i loro account G Suite for Education, gli studenti possono accedere e utilizzare i seguenti "Servizi principali" offerti da Google e descritti all'indirizzo https://gsuite.google.com/terms/user_features.html:

- Gmail
- Google+
- Calendar
- Sincronizzazione Chrome
- Classroom
- Cloud Search
- Contatti
- Documenti, Fogli, Presentazioni, Moduli
- Drive
- Gruppi
- Google Hangouts, Google Chat, Google Meet, Google Talk
- Jamboard
- Keep
- Siti
- Vault

Consentiamo inoltre agli studenti di accedere ad altri servizi Google con i loro account G Suite for Education. In particolare, vostro figlio potrebbe accedere ai seguenti "Servizi aggiuntivi": YouTube, Blogger, Google Maps, Google Takeout, Google Earth, Google Libri.

Tali applicazioni saranno attivate solo se ritenute necessarie per specifiche attività didattiche proposte dai docenti.

Nell'Informativa sulla privacy di G Suite for Education, Google fornisce informazioni sui dati che raccoglie e su come utilizza e divulga le informazioni che raccoglie dagli account G Suite for Education. È possibile consultare l'informativa online all'indirizzo https://gsuite.google.com/terms/education_privacy.html. Consigliamo di leggere l'intero documento, ma di seguito indichiamo le risposte ad alcune delle domandi più comuni.

Quali informazioni personali raccoglie Google?

Quando crea un account studente, l'I.C. Ferraris può fornire a Google determinate informazioni, tra cui, ad esempio, il nome, un indirizzo email e la password dello studente. Google può inoltre raccogliere informazioni personali direttamente dagli studenti, ad esempio la foto del profilo aggiunta all'account G Suite for Education.

Quando uno studente utilizza i servizi di Google, Google raccoglie anche le informazioni basate sull'utilizzo di tali servizi, tra cui:

- Informazioni sul dispositivo, ad esempio modello di hardware, versione del sistema operativo, identificatori univoci del dispositivo e informazioni relative alla rete mobile, incluso il numero di telefono;
- Informazioni di log, tra cui dettagli di come un utente ha utilizzato i servizi Google, informazioni sugli eventi del dispositivo e indirizzo IP (protocollo Internet) dell'utente;
- Informazioni sulla posizione ricavate tramite varie tecnologie, tra cui l'indirizzo IP, GPS e altri sensori;

- Numeri specifici delle applicazioni, come il numero di versione dell'applicazione; infine
- Cookie o tecnologie analoghe utilizzate per acquisire e memorizzare le informazioni relative a un browser o dispositivo, come la lingua preferita e altre impostazioni.

In che modo Google utilizza queste informazioni?

Nei Servizi principali di G Suite for Education, Google utilizza le informazioni personali degli studenti per fornire, gestire e proteggere i servizi. Google non pubblica annunci pubblicitari nei Servizi principali e non utilizza a scopi pubblicitari le informazioni personali raccolte nei Servizi principali.

Nei Servizi aggiuntivi, Google utilizza le informazioni raccolte in tutti i Servizi aggiuntivi per fornire, gestire, proteggere e migliorare i servizi, per svilupparne di nuovi e per proteggere Google e i suoi utenti. Google può inoltre utilizzare tali informazioni per offrire contenuti personalizzati, ad esempio risultati di ricerca più pertinenti. Google può unire le informazioni personali derivanti da un servizio a quelle (comprese le informazioni personali) di altri servizi Google.

Google utilizza le informazioni personali degli utenti delle scuole primarie e secondarie per mostrare pubblicità mirata?

No.

Per gli utenti di G Suite Education delle scuole primarie e secondarie, Google non utilizza alcun dato personale (o associato a un account G Suite for Education) per mostrare annunci pubblicitari mirati nei Servizi principali o in altri Servizi aggiuntivi a cui l'utente ha eseguito l'accesso con un account G Suite for Education.

Mio figlio può condividere informazioni con altre persone utilizzando l'account G Suite for Education?

Possiamo consentire agli studenti di accedere a servizi Google come Documenti Google e Google Sites, che includono funzioni in cui gli utenti possono condividere informazioni con altri o pubblicamente. Quando gli utenti condividono informazioni pubblicamente, queste potrebbero essere indicizzate da motori di ricerca come Google.

Gli studenti possono scrivere e ricevere mail e possono condividere file di Drive all'interno del dominio @vergaferraris.net.

Google divulga le informazioni personali di mio figlio?

Google non fornisce informazioni personali a società, organizzazioni e persone che non fanno parte di Google, ad eccezione dei seguenti casi:

- Dietro consenso del genitore o tutore. Google comunica le informazioni personali a società, organizzazioni e persone che non fanno parte di Google, che possono essere ottenute tramite le scuole che utilizzano G Suite for Education, se ha il consenso dei genitori (per i minori).

- Con l'Istituto comprensivo Ferraris di Vercelli. (Gli account G Suite for Education, in quanto account gestiti dalla scuola, consentono agli amministratori l'accesso alle informazioni in essi archiviate).
- Per elaborazione esterna Google può comunicare le informazioni personali a società affiliate o ad altre aziende o persone di fiducia di Google affinché li elaborino per conto e in base alle istruzioni di Google e nel rispetto dell'informativa sulla privacy di G Suite for Education e di eventuali altre misure appropriate relative a riservatezza e sicurezza.
- Per motivi legali Google comunica informazioni personali a società, organizzazioni o persone che non fanno parte di Google qualora ritenga in buona fede che l'accesso, l'utilizzo, la conservazione o la divulgazione di tali informazioni siano ragionevolmente necessari per:
    - Adempiere a leggi o norme vigenti, procedimenti legali o richieste governative obbligatorie.
    - Applicare i Termini di servizio vigenti, compresi gli accertamenti in merito a potenziali violazioni.
    - Individuare, prevenire o far fronte in altro modo a frodi, problemi tecnici o di sicurezza.
    - Tutelare i diritti, la proprietà o la sicurezza di Google, degli utenti di Google o del pubblico, come richiesto o consentito dalla legge.

Inoltre, Google condivide pubblicamente e con i propri partner informazioni non personali, ad esempio le tendenze di utilizzo dei propri servizi.

Quali sono le scelte a cui ho diritto come genitore o tutore?

Innanzitutto, potete autorizzare la raccolta e l'utilizzo dei dati di vostro figlio da parte di Google. Se non date il vostro consenso, non creeremo un account G Suite for Education per vostro figlio e Google non raccoglierà e non utilizzerà i dati di vostro figlio, come descritto in questa informativa. In tal caso, però, vostro figlio non potrà accedere ai servizi di GSuite for Education utilizzati dalla scuola con lo scopo di sviluppare le competenze digitali indispensabili per vivere nel XXI secolo.

Se autorizzate vostro figlio a utilizzare G Suite for Education, potete accedere o richiedere l'eliminazione dell'account G Suite for Education rivolgendovi al Dirigente dell'Istituto Comprensivo Ferraris. Se volete interrompere ogni ulteriore raccolta o utilizzo dei dati di vostro figlio potete richiederci di utilizzare i controlli del servizio disponibili per limitare l'accesso di vostro figlio a determinate funzioni o servizi oppure eliminare completamente l'account di vostro figlio. Voi e vostro figlio potete anche visitare https://myaccount.google.com dopo aver eseguito l'accesso all'account G Suite for Education per visualizzare e gestire le informazioni personali e le impostazioni dell'account.

A chi mi rivolgo se ho altre domande e dove posso trovare maggiori informazioni?

Se avete domande su come utilizziamo gli account G Suite for Education di Google o su quali scelte avete a disposizione, rivolgetevi al Dirigente scolastico e al Team digitale scrivendo al seguente indirizzo help_gsuite@vergaferraris.net.

Per ulteriori informazioni su come Google raccoglie, utilizza e divulga le informazioni personali per fornirci i servizi, invitiamo a consultare il Centro privacy di G Suite for

Education (all'indirizzo https://www.google.com/edu/trust/), l'Informativa sulla privacy di G Suite for Education (all'indirizzo https://gsuite.google.com/terms/education_privacy.html) e le Norme sulla privacy di Google (all'indirizzo https://www.google.com/intl/it/policies/privacy/).

I Servizi principali di G Suite for Education ci sono forniti ai sensi dell'Accordo G Suite for Education (all'indirizzo https://www.google.com/apps/intl/it/terms/education_terms.html)

Fac simile autorizzazione

AUTORIZZAZIONE PER UTILIZZO DELLE APPLICAZIONI E SERVIZI AGGIUNTIVI CONNESSI ALL'ACCOUNT GSUITE FOR EDUCATION

I sottoscritti _____ genitori dell'alunno _____ frequentante la classe ___ della Scuola

|_| Primaria Ferraris |_| Primaria Rodari |_| Secondaria Verga

dichiarano di aver letto l'informativa relativa all'uso di GSuite for Education e autorizzano all'uso delle applicazioni e dei servizi aggiuntivi previsti per fini didattici. Autorizzano inoltre Google a raccogliere e utilizzare le informazioni relative all'alunno esclusivamente per gli scopi descritti nell'informativa

Data _____ I genitori dell'alunno (o chi ne fa le veci)

_____

_____