Protocollo 0014264/2026 del 04/11/2026

Ministero dell'Istruzione
e del Merito

Istituto Comprensivo Statale "ALESSANDRO VOLTA"
Infanzia - Primaria - Secondaria I Grado
Via Volta, 13 - 20093 Cologno Monzese (MI) Tel. 02 25492649
Fax: 02 25492650 Cod. Mecc. MIIC8EH003 - C.F. 97632210155
E-mail:*miic8eh003@istruzione.it*
PEC: *miic8eh003@pec.istruzione.it*
Fatturazione Elettronica Codice Univoco: **UFR9XA**
Sito Web dell'istituto: www.scuolavolta.edu.it

Al personale docente, amministrativo, tecnico e ausiliario in servizio
Alla DSGA
Al sito web – sezione Privacy

Linee guida per l'utilizzo sicuro delle piattaforme cloud dell'Istituto da parte del personale docente e ATA (registro elettronico e segreteria digitale Spaggiari, piattaforme ministeriali, Google Workspace for Education)

Premessa

Le presenti linee guida costituiscono **istruzioni impartite dal titolare del trattamento** al personale autorizzato, ai sensi dell'art. 29 e dell'art. 32, par. 4, del Regolamento UE 2016/679 (di seguito GDPR) e dell'art. 2-quaterdecies del D.Lgs. 196/2003 (Codice in materia di protezione dei dati personali). Esse si applicano a tutti gli ambienti digitali in cui il personale tratta dati personali per conto dell'Istituto.

Il documento dà attuazione alle misure organizzative individuate nella **DPIA/TIA per l'adozione della piattaforma Google Workspace for Education** (prot. n. 14145/2026 del 03/11/2026) e della relativa **Integrazione sugli strumenti di intelligenza artificiale generativa** (prot. n. 14147/2026 del 03/11/2026), e richiama l'**Informativa sull'utilizzo della piattaforma Google Workspace for Education** (prot. n. 14149/2026 del 03/11/2026).

La valutazione d'impatto ha stimato come accettabili i rischi residui (accesso illegittimo ai dati: gravità 6 su 16; modifiche indesiderate e perdita di dati: 2 su 16) a condizione che gli utenti osservino le regole impartite e partecipino alle attività di formazione: il rispetto delle presenti istruzioni è, dunque, parte integrante delle misure di sicurezza adottate.

L'osservanza delle linee guida rientra negli obblighi di servizio del personale. Si richiamano in particolare gli artt. 11-bis (utilizzo delle tecnologie informatiche) e 11-ter (utilizzo dei mezzi di informazione e dei social media) del Codice di comportamento dei dipendenti pubblici (D.P.R. 62/2013, come modificato dal D.P.R. 81/2023).

In sintesi: le dodici regole essenziali

1. Le credenziali sono **personali e non cedibili**: non si comunicano a nessuno, nemmeno a colleghi o supplenti. Si attiva l'autenticazione a più fattori e si usa SPID o CIE dove disponibili.
2. Prima di lasciare la postazione, anche per pochi minuti, si **blocca lo schermo o si esce dall'account**. Sui PC d'aula e condivisi le password non si salvano nel browser.
3. Ogni dato va trattato nella **piattaforma giusta** (tabella al par. 2). PEI e documentazione sulla disabilità **non si caricano mai** su Google Workspace.

Documento informatico firmato digitalmente da INCORONATA NIGRO ai sensi del D.Lgs 82/2005 s.m.i. e norme collegate

4. Valutazioni, assenze, note e comunicazioni ufficiali alle famiglie passano **solo dal registro elettronico**.
5. Gli atti amministrativi si protocollano e si fascicolano nella **Segreteria Digitale**: Drive ed e-mail non sostituiscono il protocollo.
6. I documenti su Drive si condividono **solo con persone nominativamente individuate**. Per i documenti che contengono dati personali non si usa mai l'opzione "Chiunque abbia il link".
7. Per gli invii a più destinatari esterni si usa il campo **CCN**. Prima di premere "Invia" si verificano destinatario e allegati.
8. L'account istituzionale si usa **solo per fini di servizio**. Per comunicazioni di lavoro non si usano e-mail personali, WhatsApp o social.
9. Si usano **solo gli strumenti di IA compresi nell'ambiente istituzionale**, con l'account della scuola, e **non vi si inserisce alcun dato personale**, proprio o altrui. Ogni risultato va **verificato da una persona**.
10. Applicazioni o estensioni di terze parti non autorizzate non vanno installate. L'account istituzionale non va usato per registrarsi a servizi esterni ("*Accedi con Google*").
11. Nessuna scuola, nessun fornitore e nessun amministratore chiede mai la password per e-mail o per telefono. I **messaggi sospetti** si segnalano senza aprire link o allegati.
12. Qualunque incidente, anche solo sospetto (e-mail al destinatario sbagliato, documento condiviso per errore, dispositivo smarrito, account compromesso), si **segnala subito alla Dirigente**.

1. Ambito di applicazione e piattaforme interessate

Le linee guida si applicano a tutto il personale docente (a tempo indeterminato, determinato, supplente), al personale ATA, ai collaboratori esterni ai quali siano rilasciate credenziali istituzionali e, per quanto compatibile, al personale in servizio presso l'Istituto in posizione di comando o utilizzazione. Si applicano qualunque sia il dispositivo utilizzato (di proprietà della scuola o personale) e il luogo da cui si accede (locali scolastici, domicilio, lavoro agile).

Piattaforma	Funzioni principali	Note sul trattamento
Registro elettronico (Spaggiari)	Registro di classe e del docente, valutazioni, assenze, annotazioni e note disciplinari, scrutini, bacheca e comunicazioni scuola-famiglia, colloqui	Fornitore che opera come responsabile del trattamento ex art. 28 GDPR. Secondo la DPIA, le piattaforme ministeriali e quelle del fornitore della segreteria digitale offrono garanzie sulla collocazione in Italia dei sistemi e dei dati.
Segreteria Digitale e applicativi gestionali (Spaggiari)	Protocollo informatico, gestione documentale e fascicolazione, fascicoli di alunni e personale, contabilità e gestione amministrativa	Sede ufficiale degli atti amministrativi, secondo il Manuale di gestione documentale dell'Istituto. L'accesso avviene per profili abilitati in base alla mansione.
Piattaforme ministeriali (SIDI, Anagrafe Nazionale Studenti e relativa partizione separata, NoiPA e altre)	Adempimenti amministrativi, anagrafe degli alunni, redazione dei PEI nella partizione separata dell'ANS	Il titolare dei sistemi è il Ministero. Le credenziali sono personali e i profili sono abilitati dalla Dirigente.
Google Workspace for Education (edizione Fundamentals)	Gmail, Drive, Documenti, Fogli, Presentazioni, Moduli, Classroom, Meet, Calendar; Gemini, ove attivato dall'amministratore	Senza Data Residency non è possibile escludere trasferimenti extra UE (coperti dal Data Privacy Framework e dal Cloud Data Processing Addendum). Per questo **i dati particolari si trattano solo in caso di stretta necessità e con misure rafforzate** (DPIA/TIA).

2. Principio generale: il dato giusto nella piattaforma giusta

Il rischio principale individuato dalla DPIA non deriva dalle piattaforme in sé. Deriva dall'uso improprio di una piattaforma per finalità o tipologie di dati diverse da quelle per cui è stata adottata. La scuola privilegia le piattaforme ministeriali e quelle del fornitore della segreteria digitale. Google Workspace si usa per le funzioni collaborative, didattiche e di comunicazione che le altre piattaforme non offrono. Ciascun dipendente è tenuto ad attenersi alla seguente ripartizione, applicando i principi di minimizzazione e di limitazione della finalità (art. 5, par. 1, lett. b e c, GDPR).

Tipologia di dato o documento	Dove va trattato	Dove NON va trattato
PEI, certificazioni e diagnosi relative alla disabilità, verbali del GLO	Partizione separata dell'Anagrafe Nazionale Studenti; fascicolo riservato dell'alunno nella Segreteria Digitale	Google Workspace (Drive, Gmail, Classroom, Moduli), chat, dispositivi personali, chiavette USB
PDP, documentazione DSA e BES, dati sanitari (allergie, somministrazione farmaci, esoneri), segnalazioni ai servizi	Fascicolo riservato in Segreteria Digitale; sezioni riservate del registro elettronico, se previste e con visibilità limitata ai soli docenti del consiglio di classe	Cartelle Drive condivise, Classroom, annotazioni visibili alle famiglie, gruppi di messaggistica. Su Google Workspace solo in caso di stretta necessità, con pseudonimizzazione o cifratura (DPIA/TIA)
Valutazioni, assenze, ritardi, giustificazioni, note disciplinari, esiti degli scrutini	Registro elettronico	Fogli Google condivisi, e-mail, chat, tabelloni non autorizzati. Eventuali fogli di lavoro personali restano non condivisi e vanno riversati tempestivamente nel registro
Atti amministrativi rilevanti (istanze, provvedimenti, contratti, corrispondenza in entrata e in uscita)	Segreteria Digitale: protocollo informatico e fascicolazione, secondo il Manuale di gestione documentale	Drive come archivio definitivo, caselle e-mail personali, cartelle locali del PC
Dati del personale (assenze, congedi, certificati, procedimenti, retribuzioni)	Segreteria Digitale e piattaforme ministeriali, a cura degli uffici competenti	Google Workspace, e-mail non istituzionale, documenti condivisi tra colleghi
Verbali di organi collegiali, consigli di classe, dipartimenti, commissioni	Bozze su Documenti Google in Drive condiviso con accesso limitato ai componenti. Versione definitiva acquisita agli atti secondo le procedure dell'Istituto	Documenti personali in "Il mio Drive" condivisi con link aperto
Materiali didattici, consegne, elaborati degli alunni	Classroom e Drive istituzionale	Piattaforme esterne non autorizzate, account personali
Comunicazioni con le famiglie	Bacheca e messaggistica del registro elettronico; e-mail istituzionale	WhatsApp e altri servizi di messaggistica, social network, e-mail personale

3. Credenziali e autenticazione

Le credenziali di accesso a tutte le piattaforme sono **strettamente personali**. Il loro uso da parte di terzi è imputato al titolare dell'account. Non vanno cedute, condivise o annotate in luoghi accessibili ad altri. Il personale supplente riceve credenziali proprie e non usa quelle del docente sostituito.

La password deve essere robusta (almeno 12 caratteri, oppure una frase lunga facile da ricordare) e **diversa da quelle usate per servizi personali**. Va cambiata subito in caso di sospetta compromissione.

Qualora l'Istituto la attivi, l'**autenticazione a più fattori** è obbligatoria. Per l'accesso alle piattaforme che lo consentono si usano SPID o CIE.

Sui dispositivi condivisi (PC d'aula, LIM, laboratori, postazioni di segreteria) **non si memorizzano le password nel browser** e si usa, se possibile, la navigazione in incognito o il profilo ospite. Al termine si esegue sempre la disconnessione (logout) da tutte le piattaforme.

Nessun soggetto legittimato (Istituto, amministratori della piattaforma, Spaggiari, Google, Ministero) **chiede mai la password** per e-mail, telefono o messaggio. Le richieste di questo tipo sono tentativi di frode e vanno segnalate.

In caso di smarrimento delle credenziali di Google Workspace ci si rivolge agli amministratori all'indirizzo didattica@scuolavolta.edu.it. Per le altre piattaforme ci si rivolge alla segreteria.

4. Dispositivi, postazioni e luoghi di lavoro

4.1 Postazioni d'aula e condivise

Il registro elettronico non va mai lasciato aperto su un PC o una LIM incustoditi. Quando ci si allontana si blocca lo schermo (su Windows: tasto Windows + L). Al cambio dell'ora ci si disconnette.

Durante le lezioni **non si proietta sulla LIM** il registro, la posta elettronica o il Drive, se sono visibili valutazioni, assenze, annotazioni o dati di altri alunni. Per mostrare un contenuto si apre solo il documento necessario.

File contenenti dati personali non vanno salvati sul desktop o nelle cartelle locali dei PC d'aula. Eventuali file scaricati vanno eliminati, svuotando anche il cestino.

4.2 Dispositivi personali e lavoro da remoto

Il dispositivo personale con cui si accede alle piattaforme deve avere il **blocco schermo** attivo (PIN, password o dato biometrico), il sistema operativo e il browser aggiornati e un software antivirus attivo dove previsto. Non deve aver subito modifiche che ne riducano la sicurezza (jailbreak, root).

Su computer usati anche da familiari si accede con un profilo utente o un profilo del browser dedicato. Non si sincronizza il Drive istituzionale sul disco locale.

Si evita l'accesso da reti Wi-Fi pubbliche non protette. Se indispensabile, non si scaricano documenti con dati personali.

Le riunioni a distanza (consigli di classe, GLO, colloqui) si svolgono in un ambiente riservato, preferibilmente con auricolari, in modo che terzi non vengano a conoscenza di informazioni sugli alunni.

I dati dell'Istituto non vanno copiati su chiavette USB, dischi esterni o servizi cloud personali. Ove eccezionalmente necessario, si usano supporti cifrati forniti o autorizzati dall'Istituto.

Lo smarrimento o il furto di un dispositivo da cui si accede alle piattaforme costituisce un potenziale **data breach**. Va segnalato immediatamente e va cambiata la password di tutti gli account interessati.

4.3 Uffici di segreteria

Si adotta la regola della **scrivania pulita**: i documenti cartacei con dati personali non si lasciano incustoditi e si ritirano subito dalla stampante.

Gli schermi vanno orientati in modo da non essere visibili al pubblico allo sportello. Quando ci si allontana dalla postazione si blocca lo schermo.

5. Registro elettronico: indicazioni per i docenti

Il registro elettronico è il **documento ufficiale** dell'attività didattica. Le registrazioni (firme, assenze, argomenti delle lezioni, valutazioni) devono essere tempestive, veritiere e complete.

Prima di inserire un'annotazione si **verifica la visibilità** impostata (solo docenti, famiglia dell'alunno interessato, intera classe). Le annotazioni visibili alle famiglie devono essere oggettive, essenziali e rispettose.

Nelle annotazioni visibili, nelle note disciplinari e nelle comunicazioni **non si inseriscono**: diagnosi, informazioni sullo stato di salute, riferimenti a disabilità, DSA o BES, situazioni familiari o sociali, motivazioni

sanitarie delle assenze. Il vademecum del Garante “La scuola a prova di privacy” richiama espressamente questo divieto.

Una **nota disciplinare di classe** non deve riportare i nomi degli alunni coinvolti, perché sarebbe visibile a tutte le famiglie. I comportamenti individuali si annotano sul singolo alunno.

Nelle comunicazioni tramite bacheca si selezionano con attenzione i destinatari. Documenti riferiti a un singolo alunno si inviano solo alla relativa famiglia. Non si allegano elenchi nominativi con dati personali a comunicazioni rivolte all’intera classe.

Si accede solo ai dati delle classi e degli alunni per i quali si ha titolo in ragione dell’incarico (docenza, coordinamento, sostegno, funzioni assegnate). Esportazioni e stampe di elenchi sono ammesse solo se necessarie e vanno conservate in modo sicuro.

Gli esiti degli scrutini e degli esami si rendono disponibili secondo le indicazioni del Garante: valutazioni di dettaglio solo nell’area riservata accessibile con le credenziali dello studente o della famiglia, nessuna pubblicazione online degli esiti con voti.

6. Segreteria Digitale e gestionali: indicazioni per DSGA e assistenti amministrativi

Tutti i documenti in entrata e in uscita giuridicamente rilevanti sono **registrati nel protocollo informatico e fascicolati**, nel rispetto del Manuale di gestione documentale dell’Istituto e delle Linee guida AgID sulla formazione, gestione e conservazione dei documenti informatici. Non sono ammesse registrazioni differite o prassi non conformi al Manuale.

Ai documenti contenenti dati particolari (sanitari, relativi alla disabilità) o dati relativi a procedimenti disciplinari o giudiziari si attribuisce il **livello di riservatezza** previsto dall’applicativo, limitandone la visibilità ai soli operatori competenti.

Ciascun operatore usa esclusivamente il **proprio profilo** e le abilitazioni assegnate in base alla mansione. Le abilitazioni eccedenti o non più necessarie vanno segnalate alla DSGA.

Prima della pubblicazione all’albo online o in Amministrazione trasparente si verifica che l’atto contenga solo i dati necessari. Non si pubblicano mai dati sulla salute. Si omettono o si oscurano codici fiscali, recapiti e dati non pertinenti, secondo le Linee guida del Garante in materia di trasparenza (provv. n. 243 del 15 maggio 2014). Si rispettano i termini di pubblicazione previsti.

Nelle graduatorie e negli elenchi pubblicati non compaiono informazioni da cui si possano desumere condizioni di salute (ad esempio i benefici della L. 104/1992 alla base di precedenze).

Informazioni su alunni o personale non si forniscono per telefono o allo sportello a persone non identificate o non legittimate.

Le comunicazioni ufficiali verso soggetti esterni avvengono tramite PEO o PEC istituzionale. Per gli invii multipli si usa il campo CCN.

7. Google Workspace for Education

7.1 Account istituzionale

L’account **cognome.nome@scuolavolta.edu.it** è uno **strumento di lavoro** e va usato esclusivamente per finalità istituzionali. È vietato l’uso per fini personali, per l’accesso a social network o a servizi estranei all’attività scolastica.

Per le comunicazioni di lavoro non si usano caselle di posta personali, salvo casi di forza maggiore (art. 11-bis, D.P.R. 62/2013). Non si impostano **inoltri automatici** dalla casella istituzionale verso caselle personali.

Ogni e-mail inviata deve consentire l’identificazione del mittente e riportare un recapito istituzionale. Si raccomanda una firma con nome, qualifica e Istituto.

L'account viene cancellato al termine del servizio presso l'Istituto, con la conseguente perdita dei dati. **Prima della cessazione** ciascuno trasferisce nei Drive condivisi i documenti di interesse istituzionale e non conserva copie di dati dell'Istituto in archivi personali.

7.2 Posta elettronica

Prima di inviare si controllano **destinatari e allegati**, prestando attenzione al completamento automatico degli indirizzi, che è tra le cause più frequenti di invio errato.

Per gli invii a più destinatari esterni si usa sempre il campo **CCN**. L'uso del campo "A" o "CC" renderebbe visibili a tutti gli indirizzi altrui.

Non si allegano documenti con dati particolari. Quando è indispensabile condividerli si usa un collegamento a un file con accesso limitato ai soli destinatari autorizzati, oppure si procede tramite la segreteria.

Si diffida dei messaggi che sollecitano urgenze, chiedono credenziali o pagamenti o contengono allegati e link inattesi (**phishing**), anche se il mittente sembra noto. In caso di dubbio non si clicca e si segnala agli amministratori.

7.3 Drive e condivisione dei documenti

L'accesso generale ai file deve restare impostato su **"Con limitazioni"**. Si condivide con persone individuate nominativamente e con il ruolo minimo necessario (Visualizzatore, Commentatore, Editor).

Per i documenti che contengono dati personali **non si usa mai** l'opzione "Chiunque abbia il link". La condivisione all'esterno del dominio scolastico è ammessa solo per attività programmate e autorizzate.

I documenti di interesse istituzionale (verbali, progetti, modulistica, materiali di dipartimento) si collocano nei **Drive condivisi**, che non vanno persi alla cessazione del singolo account.

Periodicamente, e comunque a fine anno scolastico, si verificano e si revocano le condivisioni non più necessarie.

Prima di caricare un file si valuta se tutti i dati personali che contiene siano necessari. Quelli non pertinenti alla finalità del documento si eliminano o si pseudonimizzano.

7.4 Classroom

I riscontri individuali agli alunni si danno tramite commenti privati e non nello stream della classe. Valutazioni o giudizi personali non si pubblicano in spazi visibili a tutti.

Le attività che richiedono agli alunni di esporre dati particolari propri o altrui (salute, convinzioni religiose, origine, situazioni familiari) si propongono solo dopo attenta valutazione. Se possibile, si scelgono modalità alternative alla piattaforma (DPIA/TIA).

Al termine dell'anno scolastico i corsi si **archiviano**. Gli elaborati non soggetti a valutazione si cancellano di norma a fine anno. Quelli soggetti a valutazione si conservano secondo il massimario di conservazione e scarto dell'Istituto.

7.5 Meet e riunioni a distanza

Il link della riunione si diffonde solo ai partecipanti. L'organizzatore controlla gli accessi e non ammette soggetti non identificati.

Le sedute non si registrano, salvo che la registrazione sia prevista dal regolamento dell'organo collegiale o disposta dalla Dirigente, con preventiva informazione dei partecipanti. Non si effettuano registrazioni con strumenti personali.

Nelle sedute che trattano singoli alunni (consigli di classe, GLO) si condividono sullo schermo solo i documenti necessari. Si chiudono le altre finestre e le notifiche.

7.6 Moduli Google

Con i Moduli si raccolgono solo i dati strettamente necessari. Non si raccolgono dati sanitari o altri dati particolari.

Quando i compilatori appartengono all'Istituto, l'accesso si limita al dominio scolastico. Le risposte si condividono solo con chi deve elaborarle e si eliminano quando la finalità è esaurita.

7.7 Applicazioni di terze parti, estensioni e servizi aggiuntivi

Si usano esclusivamente i servizi abilitati dall'amministratore. Non risultano componenti aggiuntivi installati a livello di dominio. L'installazione da parte degli utenti è limitata alle applicazioni della lista consentita (alla data del 03/11/2026: Canva (Legacy), Mail Merge, SketchUp for School). Ogni ulteriore applicazione di terze parti o estensione collegata all'account istituzionale è ammessa solo dopo la valutazione caso per caso prevista dalla DPIA e l'autorizzazione della Dirigente.

L'account istituzionale non va usato per registrarsi a siti, app o piattaforme didattiche esterne non autorizzate (funzione "Accedi con Google"), né lo si fa usare agli alunni.

I servizi aggiuntivi di Google (ad esempio YouTube, Maps, Blogger) non si usano con gli account degli alunni, salvo specifica autorizzazione e informativa.

8. Strumenti di intelligenza artificiale

L'uso dell'intelligenza artificiale da parte del personale è disciplinato dal Regolamento UE 2024/1689 (AI Act), dalla L. 23 settembre 2025, n. 132 (in particolare artt. 11 e 14) e dalle Linee guida per l'introduzione dell'intelligenza artificiale nelle istituzioni scolastiche adottate con D.M. n. 166 del 9 agosto 2025. L'Istituto ne ha valutato l'impiego con l'**Integrazione alla DPIA – Gli strumenti di intelligenza artificiale generativa in Google Workspace for Education** (prot. n. 14147/2026 del 03/11/2026), le cui condizioni d'uso sono dettagliate in apposita circolare. Si dispone quanto segue.

Si usano **solo gli strumenti di IA generativa compresi nell'ambiente Google Workspace for Education dell'Istituto** e valutati nell'Integrazione alla DPIA (Gemini for Education, Gemini Notebook, Gemini nelle applicazioni, strumenti per i docenti in Classroom), accedendo esclusivamente con l'account istituzionale. Gli strumenti non compresi nell'ambiente istituzionale richiedono una valutazione autonoma e l'autorizzazione della Dirigente.

In nessuno strumento di IA generativa, compresi quelli istituzionali, si immettono **dati personali, propri o altrui, in qualunque forma**: il divieto è la condizione su cui si fonda la valutazione d'impatto e non ammette deroghe. La rimozione del nominativo non rende il contenuto conferibile, perché nel contesto della classe gli elementi residui consentono di norma di risalire all'interessato. Per le attività di servizio è vietato l'uso di **account personali**, anche se lo strumento ha la stessa denominazione.

L'impiego è **escluso** nella valutazione degli apprendimenti e nella formulazione di giudizi sugli alunni, nella redazione dei documenti dell'inclusione (PEI, PDP, relazioni, verbali dei GLO), nella gestione di procedimenti disciplinari e nell'adozione di determinazioni che producono effetti giuridici nei confronti di persone. Non si impiegano agenti autonomi.

L'IA ha funzione di **supporto**. I contenuti prodotti vanno **sempre verificati e validati** da chi li utilizza, che ne resta l'unico responsabile (art. 14, L. 132/2025). Valutazioni degli alunni, provvedimenti e decisioni non si affidano mai all'esito automatico di uno strumento di IA.

Nelle istituzioni scolastiche sono vietati i sistemi di riconoscimento delle emozioni (art. 5, par. 1, lett. f, AI Act). Lo stesso vale per qualsiasi uso finalizzato a profilare alunni o personale.

I contenuti prodotti si verificano prima di ogni utilizzo, con particolare riguardo a riferimenti normativi, citazioni, dati numerici e fonti. Ogni configurazione che ecceda l'uso ordinario (assistenti con finalità diverse

da quella prevista, agenti) è sottoposta prima dell'impiego al Referente per l'intelligenza artificiale o alla Dirigente.

Con gli alunni il servizio resta disattivato sulle loro utenze.

Nella scuola primaria non è previsto alcun impiego; nella secondaria è ammesso solo l'uso mediato dal docente, nell'ambito di attività da lui progettate e condotte con il proprio account, con l'IA presentata come oggetto di studio e di riflessione critica.

L'inserimento accidentale di dati personali in uno strumento di IA costituisce potenziale violazione dei dati e va segnalato subito alla Dirigente: le singole conversazioni non possono essere cancellate né dall'utente né dall'amministratore.

Ciascun dipendente partecipa alle attività di formazione predisposte dall'Istituto per assicurare un adeguato livello di alfabetizzazione in materia di IA (art. 4, AI Act).

9. Comunicazioni, messaggistica e social media

Le comunicazioni di servizio non avvengono, di norma, tramite social network o piattaforme di messaggistica pubbliche (art. 11-ter, D.P.R. 62/2013). Gli eventuali gruppi WhatsApp o simili tra genitori o tra colleghi **non sono canali istituzionali**.

In nessun gruppo di messaggistica si condividono dati personali degli alunni, valutazioni, documenti dell'Istituto, fotografie o informazioni su situazioni individuali.

Sui propri profili social il dipendente evita che le opinioni personali siano attribuibili all'Istituto. Non pubblica né diffonde documenti o informazioni conosciuti per ragioni di servizio.

Acquisizione, condivisione e pubblicazione di immagini e video degli alunni sono disciplinate dalla *Direttiva per i docenti sul trattamento delle immagini degli alunni e delle alunne*, cui si rinvia.

10. Indicazioni specifiche per collaboratori scolastici e personale tecnico

Anche i collaboratori scolastici dotati di account istituzionale osservano le regole sulle credenziali, sulla posta elettronica e sul phishing.

I collaboratori scolastici non consultano documenti o schermate lasciati incustoditi. Se notano un PC d'aula con il registro aperto o documenti abbandonati, ne informano il docente o la segreteria.

I documenti da consegnare alle famiglie o al personale si consegnano in busta chiusa al solo destinatario o a persona da questi delegata.

Il personale tecnico e gli amministratori della piattaforma usano le credenziali con privilegi amministrativi solo per le attività che le richiedono. Accedono ai contenuti degli utenti solo nei casi e con le modalità consentiti, documentando gli interventi.

11. Violazioni dei dati personali (data breach)

Il titolare deve notificare al Garante le violazioni dei dati personali entro 72 ore dal momento in cui ne viene a conoscenza (art. 33 GDPR) e, nei casi più gravi, comunicarle agli interessati (art. 34 GDPR). Questi termini si possono rispettare solo se la segnalazione interna è immediata. Nel dubbio, si segnala sempre, anche quando l'evento appare di modesta entità o è già stato risolto.

Che cosa è successo	Che cosa fare subito
E-mail o documento inviato al destinatario sbagliato	Chiedere al destinatario di cancellarlo senza ulteriore diffusione. Segnalare alla Dirigente indicando dati coinvolti, destinatari e orario.

Che cosa è successo	Che cosa fare subito
File su Drive condiviso per errore o con link aperto	Revocare immediatamente la condivisione, annotare per quanto tempo è rimasto accessibile e segnalare.
Dispositivo smarrito o rubato; chiavetta persa	Cambiare subito le password degli account usati sul dispositivo, segnalare e, se possibile, disconnettere il dispositivo dall'account Google (Gestisci account › Sicurezza › I tuoi dispositivi).
Clic su link sospetto o inserimento delle credenziali in una pagina fraudolenta	Cambiare subito la password, verificare l'autenticazione a più fattori e segnalare agli amministratori e alla Dirigente. Non cancellare il messaggio, che serve per l'analisi.
Accessi anomali, modifiche o cancellazioni inattese di dati nel registro o in Drive	Non intervenire per correggere prima di aver segnalato. Annotare quanto osservato e segnalare immediatamente.

La segnalazione si effettua alla **Dirigente Scolastica**, per e-mail istituzionale e, nei casi urgenti, anche per telefono. La Dirigente coinvolge il Responsabile della Protezione dei Dati (dpo@vargiuscuola.it), valuta la necessità di notifica al Garante e di comunicazione agli interessati e documenta l'evento nel registro delle violazioni (art. 33, par. 5, GDPR), secondo la Procedura per la gestione delle violazioni dei dati personali adottata dall'Istituto, cui si rinvia per modulistica e tempi. Chi segnala tempestivamente un proprio errore collabora alla tutela degli interessati: la tempestività della segnalazione è valutata positivamente.

12. Verifiche, formazione e aggiornamento

Gli amministratori delle piattaforme possono verificare il corretto utilizzo degli account e, in caso di attività anomale, sospenderli o revocarli, come indicato nell'Informativa. Le verifiche sono finalizzate alla sicurezza dei sistemi e alla tutela dei dati e si svolgono nel rispetto dell'art. 4 della L. 300/1970 e dell'art. 114 del Codice, senza controllo a distanza dell'attività lavorativa.

Il personale è tenuto a partecipare alle attività di formazione e sensibilizzazione sulla protezione dei dati, sulla sicurezza informatica e sull'uso dell'IA promosse dall'Istituto. Tali attività sono condizione per mantenere contenuto il rischio residuo stimato dalla DPIA.

Le presenti linee guida sono aggiornate in occasione della revisione periodica della DPIA/TIA, di modifiche normative o tecnologiche rilevanti o dell'attivazione di nuovi servizi.

Per chiarimenti ci si rivolge alla Dirigente Scolastica, agli amministratori della piattaforma (didattica@scuolavolta.edu.it) o al Responsabile della Protezione dei Dati (dpo@vargiuscuola.it).

13. Riferimenti normativi e documentali

– Regolamento UE 2016/679 (GDPR), in particolare artt. 5, 9, 24, 25, 28, 29, 32, 33, 34, 35, 44-46.

– D.Lgs. 30 giugno 2003, n. 196, come modificato dal D.Lgs. 101/2018, in particolare artt. 2-sexies, 2-quaterdecies e 114.

– D.P.R. 16 aprile 2013, n. 62 (Codice di comportamento dei dipendenti pubblici), come modificato dal D.P.R. 13 giugno 2023, n. 81: artt. 11-bis e 11-ter.

– D.Lgs. 7 marzo 2005, n. 82 (Codice dell'Amministrazione Digitale) e Linee guida AgID sulla formazione, gestione e conservazione dei documenti informatici.

– D.L. 6 luglio 2012, n. 95, conv. con L. 135/2012, art. 7 (registro elettronico e servizi online scuola-famiglia).

– Regolamento unico per le infrastrutture e i servizi cloud per la PA, adottato dall'Agenzia per la Cybersicurezza Nazionale con decreto direttoriale n. 21007/24 del 27 giugno 2024.

– Regolamento UE 2024/1689 (AI Act), artt. 4 e 5; L. 23 settembre 2025, n. 132, artt. 11 e 14; D.M. 9 agosto 2025, n. 166 (Linee guida per l'introduzione dell'IA nelle istituzioni scolastiche).

– D.I. 29 dicembre 2020, n. 182, come modificato dal D.I. 1° agosto 2023, n. 153, e nota MIM prot. n. 2780 del 12 giugno 2023 (redazione dei PEI nella partizione separata dell'ANS).

– Garante per la protezione dei dati personali: vademecum "La scuola a prova di privacy" (edizione aggiornata 2025); Linee guida in materia di trasparenza sul web (provv. n. 243 del 15 maggio 2014).

– EDPB, "2022 Coordinated Enforcement Action – Use of cloud-based services by the public sector" (17 gennaio 2023).

- **Documenti dell'Istituto**: DPIA/TIA Google Workspace for Education (prot. n. 14145/2026); Informativa sull'utilizzo della piattaforma (prot. n. 14149/2026); Manuale di gestione documentale pubblicato in Amministrazione Trasparente con Decreto 8339/2025 del 30/06/2025; Regolamento per la gestione dei data breach; DIRETTIVA sul trattamento delle immagini degli alunni (prot. n.11255/2026).

LA DIRIGENTE SCOLASTICA

Prof.ssa Incoronata Nigro

Documento informatico firmato digitalmente ai sensi del c.d. Codice dell'Amministrazione Digitale e normativa connessa.