ISTRUZIONI OPERATIVE / VADEMECUM

per l'uso responsabile dell'Intelligenza Artificiale



Finalità del documento

Il presente vademecum traduce in indicazioni pratiche il Regolamento d'Istituto sull'uso responsabile dell'Intelligenza Artificiale. L'obiettivo è consentire al personale di utilizzare gli strumenti di IA in modo utile, controllato, sicuro e conforme alla normativa in materia di protezione dei dati personali, evitando comportamenti che possano esporre studenti, famiglie, personale o Istituto a rischi non necessari.

Campo	Indicazione
Versione	00
Data	25.05.2026
Riferimento interno	Regolamento d'Istituto sull'uso responsabile dell'IA e relative appendici operative
Ambito	Attività didattiche, amministrative, organizzative e comunicazioni riconducibili all'Istituto
Documento destinato a	Docenti, assistenti amministrativi, DSGA, personale ATA e altri soggetti autorizzati

Documento operativo interno - da diffondere al personale e da conservare agli atti dell'Istituto

Indice

- 1. Scopo, destinatari e criterio generale di prudenza
- 2. Le dieci regole essenziali da applicare sempre
- 3. Cosa si intende per IA e quali strumenti rientrano nel vademecum
- 4. Strumenti consentiti, whitelist e richiesta di autorizzazione
- 5. Dati personali: cosa non deve mai essere inserito nei prompt
- 6. Regole operative per i docenti
- 7. Regole operative per assistenti amministrativi e segreteria
- 8. Account, credenziali, impostazioni privacy e sicurezza informatica
- 9. Verifica degli output, fonti, diritto d'autore e integrità professionale
- 10. Attività con gli studenti e prevenzione degli usi impropri
- 11. Divieti, impieghi ad alto impatto e casi che richiedono autorizzazione rafforzata
- 12. Incidenti, data breach, errori di caricamento e segnalazioni
- 13. Esempi pratici di prompt corretti e non corretti
- 14. Check-list operative per docenti e uffici amministrativi

Avvertenza di lettura

Il vademecum non sostituisce il Regolamento d'Istituto, le informative privacy, le procedure interne, le istruzioni del Dirigente Scolastico e del DSGA, né eventuali specifiche condizioni d'uso degli strumenti autorizzati. In caso di dubbio operativo, si applica il principio di maggiore cautela: ***non caricare dati personali, non usare strumenti non approvati e chiedere indicazioni al referente interno competente.***

1. Scopo, destinatari e criterio generale di prudenza

Le presenti istruzioni operative sono rivolte a tutto il personale dell'Istituto che, nello svolgimento delle proprie mansioni, intenda utilizzare strumenti di Intelligenza Artificiale per attività didattiche, amministrative, organizzative o di supporto alla comunicazione istituzionale. Rientrano tra i destinatari, in particolare, i docenti, gli assistenti amministrativi, il personale ATA, i referenti di progetto, il DSGA e ogni altro soggetto autorizzato a operare per conto dell'Istituto. L'IA può essere un valido ausilio per predisporre bozze, semplificare testi, organizzare materiali, generare esempi, supportare attività di studio, analizzare contenuti non riservati e migliorare l'efficienza del lavoro. Tuttavia, l'IA non è un soggetto responsabile, non sostituisce il personale scolastico e non può assumere decisioni in luogo dell'Istituto.

Il criterio generale da seguire è semplice: l'IA può essere utilizzata solo come strumento di supporto, mai come destinatario incontrollato di informazioni riservate e mai come sostituto del giudizio professionale umano. Ogni contenuto prodotto o rielaborato mediante IA deve essere verificato, adattato al contesto scolastico e validato dalla persona che lo utilizza.

Regola di prudenza

Prima di usare uno strumento IA chiedersi sempre: lo strumento è autorizzato? Sto inserendo dati personali o informazioni riservate? L'output sarà controllato da una persona competente prima dell'uso? Se anche una sola risposta non è chiara, l'attività deve essere sospesa e sottoposta a verifica interna.

2. Le dieci regole essenziali da applicare sempre

Le seguenti regole costituiscono la sintesi operativa minima. Devono essere applicate in ogni attività, anche quando lo strumento sembra semplice, gratuito o già disponibile online.

1. Utilizzare solo strumenti IA preventivamente autorizzati dall'Istituto e inseriti nella whitelist o comunque approvati per la specifica attività.
2. Non inserire nei prompt dati personali di studenti, famiglie o personale, salvo specifica autorizzazione e solo con strumenti idonei sotto il profilo privacy e sicurezza.
3. Non caricare documenti riservati, atti protocollati, elenchi nominativi, registri, certificazioni sanitarie, PEI, PDP, relazioni o provvedimenti disciplinari su strumenti non autorizzati.
4. Preferire sempre dati anonimi, fittizi, aggregati o esempi costruiti ad hoc, soprattutto nelle attività didattiche.
5. Verificare sempre l'output: l'IA può inventare informazioni, citazioni, riferimenti normativi, fonti, date, nomi e contenuti tecnici.
6. Non affidare all'IA decisioni su valutazioni, voti, ammissioni, provvedimenti disciplinari, percorsi individualizzati o gestione di situazioni delicate.
7. Non usare l'IA per sorvegliare, profilare, classificare o inferire emozioni, fragilità, rendimento, comportamento o caratteristiche personali degli studenti.
8. Non generare, diffondere o tollerare contenuti lesivi, discriminatori, manipolati, falsi, offensivi, deepfake o comunque idonei a ledere dignità, reputazione o riservatezza di persone.
9. Proteggere account e credenziali: usare account istituzionali ove previsti, password robuste, autenticazione a più fattori ove disponibile e impostazioni che limitino cronologia e uso dei dati per addestramento.
10. Segnalare tempestivamente errori, caricamenti accidentali di dati, usi impropri, sospetti incidenti o criticità al Dirigente/DSGA/referente indicato dalla scuola, secondo la procedura interna.

3. Cosa si intende per IA e quali strumenti rientrano nel vademecum

Ai fini operativi, per strumenti di IA si intendono tutti i sistemi che, con diversi livelli di autonomia, generano o rielaborano contenuti a partire da input dell'utente. Possono produrre testi, immagini, audio, video, codice, sintesi, traduzioni, mappe concettuali, quiz, presentazioni, analisi di documenti, suggerimenti o classificazioni. Rientrano nel presente vademecum, a titolo esemplificativo: chatbot generativi, strumenti di scrittura assistita, correttori avanzati, generatori di immagini, strumenti di sintesi di documenti, piattaforme didattiche con funzioni IA, estensioni del browser, assistenti integrati in suite di produttività, sistemi di trascrizione o traduzione automatica, strumenti che analizzano file caricati dall'utente e agenti IA in grado di compiere azioni su altri servizi. Non rileva il fatto che lo strumento sia gratuito, a pagamento, integrato in un servizio già utilizzato o disponibile tramite account personale. Se lo strumento tratta input forniti dal personale e restituisce output generati o rielaborati automaticamente, deve essere valutato secondo le regole dell'Istituto.

Categoria	Descrizione operativa	Esempio pratico	Cautela richiesta
A - Basso rischio	Uso guidato, senza account degli studenti e senza dati personali.	Generazione di esempi fittizi, esercizi, tracce, domande di ripasso.	Verifica dell'output e divieto di inserire dati reali.
B - Rischio medio	Uso didattico con account individuali o contenuti riconducibili agli studenti.	Piattaforma didattica con profili nominativi o elaborati individuali.	Valutazione preventiva, istruzioni specifiche e minimizzazione dei dati.
C - Rischio medio-alto	Uso amministrativo o istituzionale su processi/documenti dell'Istituto.	Bozze di comunicazioni, supporto a procedure di ufficio, rielaborazioni interne.	Verifica contrattuale, sicurezza, tracciabilità e autorizzazione interna.
D - Alto impatto	Automazioni, agenti IA, integrazioni con sistemi scolastici o impieghi	Agente che invia email, accede ad archivi o interagisce con	Autorizzazione rafforzata, misure tecniche specifiche e

Categoria	Descrizione operativa	Esempio pratico	Cautela richiesta
	potenzialmente invasivi.	gestionali.	coinvolgimento delle funzioni competenti.

4. Strumenti consentiti, whitelist e richiesta di autorizzazione

Per attività riconducibili all'Istituto devono essere utilizzati esclusivamente strumenti IA preventivamente approvati e inseriti nell'elenco degli strumenti autorizzati. La presenza di uno strumento nella whitelist non equivale a libertà di uso illimitato: ogni strumento deve essere utilizzato solo per le finalità, con i limiti e secondo le impostazioni indicate nella relativa scheda di approvazione.

Prima di introdurre un nuovo strumento, il docente o l'ufficio interessato deve compilare la richiesta interna prevista dal Regolamento, indicando almeno: nome dello strumento, fornitore, finalità, categoria di rischio, dati eventualmente trattati, account richiesti, impostazioni privacy disponibili, integrazioni con sistemi scolastici e periodo di utilizzo. La valutazione non è un adempimento formale, ma un presidio di tutela: serve a verificare se lo strumento è coerente con le finalità scolastiche, se tratta dati personali, se trasferisce dati fuori dallo Spazio Economico Europeo, se consente di disattivare l'uso dei dati per addestramento, se conserva prompt e file caricati, se prevede adeguate misure di sicurezza e se richiede ulteriori adempimenti privacy.

Uso di strumenti personali

L'utilizzo di account personali per attività dell'Istituto è da evitare. Quando sono previsti account, devono essere preferiti account istituzionali e configurazioni gestite o comunque approvate dalla scuola. Non è consentito aggirare la whitelist usando account privati, dispositivi personali o versioni gratuite di strumenti non valutati.

5. Dati personali: cosa non deve mai essere inserito nei prompt

Il prompt e i file caricati in uno strumento IA possono essere trattati dal fornitore del servizio secondo condizioni tecniche e contrattuali non sempre controllabili dalla scuola. Per questo motivo è vietato inserire dati personali non necessari, informazioni riservate o contenuti che rendano identificabili studenti, famiglie o personale, salvo diversa autorizzazione specifica e documentata.

È necessario considerare dato personale non solo il nome e cognome, ma qualsiasi informazione che, direttamente o indirettamente, consenta di identificare una persona: classe frequentata, iniziali, dettagli familiari, descrizioni troppo specifiche, fotografie, registrazioni, codici identificativi, indirizzi, recapiti, annotazioni comportamentali o valutative.

Non inserire	Perché è rischioso	Alternativa corretta
Nomi, cognomi, iniziali, fotografie, video o audio di studenti	Rendono identificabile il minore e possono essere conservati o riutilizzati dallo strumento.	Usare nomi fittizi, casi inventati o descrizioni generiche.
PEI, PDP, certificazioni sanitarie, diagnosi, DSA, disabilità, dati di salute	Sono dati particolari e richiedono tutele rafforzate; l'uso in strumenti non autorizzati è vietato.	Formulare domande generali senza riferimenti al caso reale.
Note disciplinari, relazioni riservate, segnalazioni, situazioni familiari	Possono ledere riservatezza e dignità degli interessati.	Chiedere supporto su uno schema astratto o su una traccia neutra.

Non inserire	Perché è rischioso	Alternativa corretta
Elenchi alunni, registri, voti nominativi, presenze, assenze	Sono dati scolastici riconducibili a persone identificabili.	Usare dati aggregati o fittizi, se necessari per esempi tecnici.
Atti protocollati, documenti amministrativi riservati, bozze contenenti dati reali	Possono uscire dal perimetro di controllo dell'Istituto.	Rimuovere dati identificativi o lavorare solo con strumenti approvati per uso amministrativo.
Credenziali, password, link riservati, token, codici di accesso	Espongono l'Istituto a rischio di accesso abusivo e compromissione dei sistemi.	Non inserirli mai. Gestirli esclusivamente con canali e strumenti autorizzati.

Anonimizzazione effettiva

Sostituire il nome con iniziali o con espressioni come "lo studente della 2B con diagnosi..." non sempre rende anonimo il contenuto. Se il contesto permette comunque di risalire alla persona, il dato resta personale. L'anonimizzazione deve essere reale, non apparente.

6. Regole operative per i docenti

I docenti possono utilizzare strumenti IA autorizzati come supporto alla progettazione didattica, alla predisposizione di materiali, alla semplificazione di testi, alla generazione di esempi, alla creazione di rubriche valutative generiche, alla preparazione di attività laboratoriali o alla revisione linguistica di contenuti non riservati. L'uso deve restare coerente con la libertà di insegnamento, con il PTOF, con le indicazioni del Consiglio di classe e con le regole interne sulla protezione dei dati.

Nella didattica, l'IA deve essere presentata agli studenti come strumento da comprendere e governare criticamente, non come scorciatoia per sostituire studio, ricerca, riflessione personale o produzione originale. È opportuno che il docente chiarisca preventivamente quando l'IA può essere usata, per quali fasi del lavoro, con quali limiti e con quale obbligo di dichiarazione.

Attività docente	Uso generalmente ammissibile	Limite da rispettare
Preparazione lezioni	Generare scalette, esempi, esercizi, domande guida, attività di recupero o potenziamento.	Controllare accuratezza, adeguatezza all'età e coerenza con il curricolo.
Materiali didattici	Semplificare testi, creare glossari, proporre esempi fittizi, predisporre quiz.	Non caricare materiali protetti o riservati se non autorizzati; citare le fonti quando necessario.
Valutazione	Predisporre griglie generiche o criteri astratti di valutazione.	Non far decidere all'IA voti, giudizi individuali, promozioni o provvedimenti; la valutazione resta del docente.
Correzione elaborati	Ricevere suggerimenti generali su chiarezza, struttura o grammatica, se consentito e senza dati identificativi.	Non caricare compiti nominativi, elaborati con dati personali o verifiche riconducibili a studenti su strumenti non autorizzati.
Inclusione	Creare materiali facilitati, mappe	Non inserire dati su disabilità,

Attività docente	Uso generalmente ammissibile	Limite da rispettare
	concettuali generiche o esercizi graduati.	diagnosi, PEI/PDP o situazioni personali dello studente.
Comunicazioni	Predisporre bozze generiche di avvisi o testi informativi.	Rileggere, adattare e validare; non inserire dati personali o casi specifici.

Quando il docente consente l'uso dell'IA agli studenti, deve esplicitare le condizioni dell'attività: finalità, strumenti ammessi, parti del lavoro in cui l'IA può essere utilizzata, modalità di dichiarazione dell'uso, obbligo di verifica delle fonti e conseguenze dell'uso non dichiarato o scorretto. È opportuno valorizzare attività che chiedano allo studente di motivare scelte, confrontare fonti, spiegare il processo seguito e distinguere il contributo personale dall'eventuale supporto dello strumento.

Valutazione e responsabilità docente

L'IA non deve essere utilizzata come correttore automatico decisionale. Può supportare la costruzione di rubriche o la revisione di testi anonimi, ma non può sostituire il giudizio professionale del docente né trattare dati degli studenti in assenza di idonea autorizzazione.

7. Regole operative per assistenti amministrativi e segreteria

L'uso dell'IA in ambito amministrativo richiede particolare cautela, perché gli uffici trattano quotidianamente dati personali, dati particolari, documenti riservati, atti protocollati e informazioni non destinate alla diffusione. Gli assistenti amministrativi possono utilizzare strumenti IA solo se autorizzati e solo per le finalità indicate dall'Istituto o dal DSGA/Dirigente Scolastico. Sono generalmente ammissibili, con strumenti autorizzati e senza inserimento di dati personali reali, attività come: predisposizione di bozze neutre, semplificazione linguistica di testi generali, organizzazione di scalette, redazione di modelli standard, sintesi di normative pubbliche, creazione di check-list interne e supporto alla comprensione di documentazione non riservata. Anche in questi casi, l'output deve essere sempre verificato dalla persona incaricata.

Attività amministrativa	Indicazione operativa	Divieto/attenzione
Bozze di circolari o comunicazioni	Usare prompt generici, senza nomi, casi individuali o allegati riservati.	Non inviare o pubblicare testi generati senza revisione umana e validazione interna.
Supporto a modulistica	Chiedere schemi, elenchi di campi, bozze standard, check-list.	Non caricare moduli compilati, documenti firmati o protocollati contenenti dati reali.
Sintesi documenti pubblici	Usare testi pubblici o riferimenti normativi non riservati, verificando sempre le fonti.	Non affidarsi a riferimenti normativi generati senza controllo.
Gestione alunni e famiglie	Evitare l'uso IA salvo strumenti formalmente approvati per il processo specifico.	Non inserire dati su iscrizioni, assenze, voti, salute, disabilità, procedimenti, contenziosi.
Personale scolastico	Usare solo modelli generici e dati fittizi.	Non caricare fascicoli, contratti, procedimenti disciplinari, assenze, certificati o dati sanitari.

Attività amministrativa	Indicazione operativa	Divieto/attenzione
Protocollo e archivi	Non usare strumenti IA esterni per trattare atti d'archivio salvo autorizzazione specifica.	Non caricare documenti protocollati, file riservati, allegati o scansioni contenenti dati personali.

Gli uffici devono prestare attenzione anche alla sicurezza delle informazioni: un documento apparentemente generico può contenere metadati, firme, numeri di protocollo, riferimenti a fascicoli o informazioni indirettamente identificative. Prima di ogni eventuale uso, i contenuti devono essere depurati da dati personali e riservati. Se tale operazione non è possibile o non è sicura, lo strumento IA non deve essere utilizzato.

Regola per la segreteria

Nel dubbio, un documento amministrativo reale non deve essere caricato su strumenti IA. Per ottenere supporto, descrivere il problema in modo astratto e usare esempi fittizi. Gli atti ufficiali restano soggetti alle procedure ordinarie di istruttoria, firma, protocollo, pubblicazione e conservazione.

8. Account, credenziali, impostazioni privacy e sicurezza informatica

L'uso dell'IA deve avvenire con adeguate misure di sicurezza. Gli account utilizzati per attività scolastiche devono essere, ove possibile, istituzionali e non personali. Le credenziali non devono essere condivise tra colleghi, studenti o soggetti esterni. Ogni utente è responsabile dell'uso del proprio account e deve adottare password robuste, diverse da quelle usate per altri servizi, nonché l'autenticazione a più fattori quando disponibile.

Prima di utilizzare uno strumento autorizzato, occorre verificare le impostazioni richieste dalla scheda interna: disattivazione della cronologia ove prevista, esclusione dell'uso dei prompt per addestramento ove disponibile, limitazione della condivisione dei contenuti, controllo dei permessi di accesso, gestione dei file caricati e cancellazione dei contenuti non più necessari.

Particolare attenzione deve essere prestata alle estensioni del browser e agli strumenti integrati in applicazioni di uso quotidiano. Alcune estensioni possono leggere pagine web, email, documenti aperti o contenuti copiati negli appunti. L'installazione di estensioni, componenti aggiuntivi, plugin o integrazioni con servizi cloud deve essere autorizzata secondo le regole tecniche dell'Istituto.

Misura	Comportamento richiesto
Password	Utilizzare password robuste, non riutilizzate e non condivise. Non inserirle mai nei prompt.
Autenticazione a più fattori	Attivarla quando disponibile, soprattutto per account istituzionali o servizi collegati a documenti scolastici.
Cronologia e addestramento	Disattivare, ove previsto, la cronologia e l'uso dei contenuti per migliorare/addestrare il servizio.
File caricati	Caricare solo file non riservati e autorizzati. Cancellare i file quando non servono più, se lo strumento lo consente.
Condivisione output	Non condividere link pubblici o conversazioni contenenti informazioni interne.

Misura	Comportamento richiesto
Dispositivi	Evitare l'uso da dispositivi non protetti. Bloccare lo schermo e mantenere aggiornati browser e sistemi.
Estensioni e plugin	Installare solo componenti approvati. Non concedere permessi ampi senza valutazione tecnica.

9. Verifica degli output, fonti, diritto d'autore e integrità professionale

Gli strumenti IA possono produrre testi molto convincenti ma inesatti. Possono inventare citazioni, riferimenti normativi, sentenze, dati statistici, bibliografie, link e contenuti tecnici. Per questo motivo nessun output deve essere utilizzato in modo automatico, soprattutto se destinato a studenti, famiglie, sito web, albo, amministrazione trasparente, atti interni o comunicazioni ufficiali.

Ogni output deve essere sottoposto a controllo umano: coerenza con il contesto scolastico, correttezza giuridica o tecnica, completezza, tono comunicativo, assenza di discriminazioni o stereotipi, rispetto della normativa privacy, conformità alle procedure interne, rispetto del diritto d'autore e correttezza delle fonti.

Per i materiali didattici è necessario prestare attenzione all'originalità del contenuto, alla citazione delle fonti e all'eventuale uso di opere protette. L'IA non deve essere utilizzata per aggirare regole su plagio, copyright, citazioni, licenze o correttezza accademica. Quando l'output si basa su fonti esterne, il docente o l'ufficio deve verificare direttamente tali fonti e non limitarsi a riportare quanto generato dallo strumento.

Controllo minimo prima dell'uso

Prima di utilizzare un testo prodotto con IA verificare: destinatario, dati personali presenti, fonti, riferimenti normativi, tono, completezza, coerenza con circolari e regolamenti dell'Istituto, eventuali effetti sugli interessati. La responsabilità finale resta sempre della persona che usa il contenuto.

10. Attività con gli studenti e prevenzione degli usi impropri

L'educazione all'uso consapevole dell'IA rientra nelle competenze digitali e nella cittadinanza digitale. Gli studenti devono essere aiutati a comprendere potenzialità e limiti degli strumenti, i rischi di errore, manipolazione, disinformazione, violazione della privacy, plagio e dipendenza da output automatici.

Nelle attività didattiche, il docente deve chiarire in anticipo se l'uso dell'IA è consentito, vietato o consentito solo per determinate fasi. Ad esempio, può essere ammesso per generare idee iniziali, ottenere una spiegazione alternativa o costruire una scaletta, ma non per consegnare un elaborato interamente prodotto dallo strumento senza rielaborazione personale e senza dichiarazione.

Deve essere vietato e tempestivamente segnalato ogni uso dell'IA finalizzato a deridere, manipolare, imitare, diffamare, minacciare o danneggiare studenti, docenti, personale o terzi. Particolare attenzione va posta a immagini sintetiche, fotomontaggi, deepfake, audio falsi, profili falsi, messaggi offensivi o contenuti sessualizzati o discriminatori. Tali condotte possono integrare violazioni disciplinari e, nei casi più gravi, profili di responsabilità ulteriori.

Scenario	Indicazione per il docente
Compito scritto a casa	Specificare se l'IA è ammessa e chiedere, se del caso, una breve dichiarazione dell'uso fatto.
Verifica in classe	Se l'uso non è previsto, impedirlo con regole chiare e vigilanza ordinaria, evitando strumenti invasivi non autorizzati.

Scenario	Indicazione per il docente
Lavoro di gruppo	Far documentare fonti, passaggi decisionali e contributo personale dei componenti.
Produzione multimediale	Vietare l'uso di immagini, voci o video riconducibili a persone reali senza presupposti e autorizzazioni adeguate.
Educazione civica digitale	Affrontare privacy, attendibilità delle fonti, bias, manipolazione, rispetto della dignità e responsabilità online.

11. Divieti, impieghi ad alto impatto e casi che richiedono autorizzazione rafforzata

Nel contesto scolastico sono vietati gli usi dell'IA sproporzionati, invasivi o non coerenti con la finalità educativa e istituzionale. Sono inoltre vietate le pratiche non consentite dalla normativa, dalle disposizioni interne o dalle istruzioni del Dirigente Scolastico.

- **Profilazione e decisioni automatizzate:** non utilizzare strumenti IA per classificare studenti, prevedere rendimento, assegnare voti, decidere provvedimenti, ammissioni o percorsi individuali senza controllo umano e senza base giuridica adeguata.
- **Riconoscimento biometrico:** non utilizzare riconoscimento facciale, vocale o altre tecnologie biometriche per identificare studenti o personale, salvo casi espressamente autorizzati e valutati secondo legge.
- **Inferenza emotiva:** non usare strumenti che pretendono di rilevare emozioni, attenzione, stress, affidabilità o stati interiori degli studenti.
- **Sorveglianza invasiva:** non utilizzare IA per monitoraggi occulti, tracciamenti non necessari, controllo sistematico delle attività o analisi comportamentali non autorizzate.
- **Dati particolari:** non trattare tramite IA dati su salute, disabilità, PEI/PDP, origine, convinzioni, situazioni familiari o altri dati delicati senza istruttoria specifica.
- **AI agent e automazioni:** non attivare agenti che inviano email, modificano documenti, accedono a gestionali, aprono ticket, interagiscono con archivi o compiono azioni in autonomia senza autorizzazione rafforzata.

Gli impieghi ad alto impatto devono essere sottoposti a valutazione preventiva, con il coinvolgimento delle funzioni competenti e, ove necessario, del DPO. In tali casi possono essere richieste misure ulteriori, quali analisi dei rischi, verifica contrattuale, istruzioni specifiche agli autorizzati, tracciamento delle attività, limitazione degli accessi, valutazione d'impatto e informazione agli interessati.

12. Incidenti, data breach, errori di caricamento e segnalazioni

Può accadere che, per errore, vengano inseriti in uno strumento IA dati personali, documenti riservati o informazioni non destinate alla condivisione. In questi casi non bisogna minimizzare l'evento né tentare di gestirlo individualmente senza informare l'Istituto. La tempestività è essenziale per contenere il rischio e valutare gli adempimenti necessari. Devono essere segnalati immediatamente: caricamento accidentale di dati personali o documenti riservati; condivisione non autorizzata di conversazioni o output; perdita di credenziali; uso di account compromessi; generazione o diffusione di contenuti lesivi; casi di deepfake o cyberbullismo; installazione non autorizzata di plugin; comportamenti anomali dello strumento; sospetto accesso di terzi a file o prompt.

Fase	Cosa fare
1. Interrompere	Sospendere l'uso dello strumento e non proseguire con ulteriori caricamenti o condivisioni.
2. Conservare le informazioni essenziali	Annotare data, ora, strumento usato, account, contenuto coinvolto, persone potenzialmente interessate e azioni già compiute.
3. Non cancellare in modo impulsivo	Se possibile, evitare azioni che impediscano la ricostruzione dell'evento; seguire le istruzioni del referente interno.
4. Segnalare subito	Informare Dirigente/DSGA/referente privacy o informatico secondo la procedura interna dell'Istituto.
5. Collaborare	Fornire le informazioni necessarie per valutare rischio, misure di contenimento ed eventuali comunicazioni agli interessati o all'Autorità.

Tempestività

Un possibile data breach deve essere gestito senza ritardo. La segnalazione interna non serve ad attribuire colpe, ma ad attivare le misure di contenimento, documentare l'evento e tutelare gli interessati e l'Istituto.

13. Esempi pratici di prompt corretti e non corretti

Gli esempi che seguono mostrano come trasformare richieste rischiose in richieste più sicure. Le formulazioni vanno sempre adattate allo strumento autorizzato e alle istruzioni interne.

Obiettivo	Prompt da evitare	Prompt più corretto
Materiale inclusivo	"Prepara esercizi per Mario Rossi, alunno con DSA della 2A, sulla base del suo PDP allegato".	"Prepara tre esercizi graduati di grammatica per una classe seconda della scuola secondaria, con consegne brevi e linguaggio semplice. Usa un caso fittizio."
Comunicazione a famiglia	"Scrivi una mail ai genitori di Giulia Bianchi perché ha avuto una nota disciplinare per..."	"Predisponi una bozza generica di comunicazione scuola-famiglia relativa a un colloquio richiesto per motivi didattico-educativi, senza dati personali."
Circolare	"Rielabora questa circolare protocollata con allegati contenenti nominativi".	"Predisponi una bozza di circolare generale sul calendario degli incontri, senza riferimenti a persone o documenti riservati."
Sintesi normativa	"Dimmi cosa prevede la norma e dammi i riferimenti" senza verifica successiva.	"Indicami una scaletta dei profili da verificare su questo tema. I riferimenti normativi saranno controllati su fonti ufficiali prima dell'uso."

Obiettivo	Prompt da evitare	Prompt più corretto
Valutazione elaborato	"Assegna un voto a questo compito di Luca".	"Suggerisci una griglia generale di valutazione per un elaborato argomentativo di scuola secondaria, con criteri e livelli descrittivi."
Segreteria	"Analizza questo file Excel con nominativi, assenze e certificati".	"Crea una check-list generale per controllare la completezza di una pratica amministrativa, usando campi fittizi."

Un buon prompt scolastico dovrebbe essere chiaro nella finalità, privo di dati personali, basato su esempi fittizi, limitato allo scopo, orientato a ottenere una bozza o uno schema e non una decisione definitiva. È utile specificare: destinatari, tono, livello scolastico, lunghezza desiderata, vincoli di linguaggio, necessità di evitare dati personali e obbligo di fornire contenuti verificabili.

14. Check-list operative per docenti e uffici amministrativi

Le seguenti check-list possono essere utilizzate prima di ogni attività con strumenti IA. Non sostituiscono le procedure interne, ma aiutano a ridurre il rischio di errori operativi.

Check-list docenti	Esito
Lo strumento è autorizzato per la finalità didattica prevista?	[ ] Sì [ ] No
Il prompt è privo di dati personali, dati particolari e riferimenti identificativi?	[ ] Sì [ ] No
L'attività con gli studenti è stata spiegata con regole chiare su uso consentito e dichiarazione?	[ ] Sì [ ] No
L'output sarà verificato prima di essere usato o condiviso?	[ ] Sì [ ] No
Sono state controllate fonti, accuratezza, tono, inclusività e coerenza con il curricolo?	[ ] Sì [ ] No
È escluso che l'IA assuma decisioni valutative individuali?	[ ] Sì [ ] No

Check-list assistenti amministrativi/segreteria	Esito
Lo strumento è autorizzato per uso amministrativo e per la specifica attività?	[ ] Sì [ ] No
Non sono stati caricati atti protocollati, fascicoli, elenchi, certificati o documenti riservati?	[ ] Sì [ ] No
Il testo inserito è generico, anonimizzato in modo effettivo o fittizio?	[ ] Sì [ ] No

Check-list assistenti amministrativi/segreteria	Esito
Le impostazioni privacy e sicurezza richieste sono state applicate?	[ ] Sì [ ] No
L'output sarà controllato da personale competente prima di uso, invio, firma o pubblicazione?	[ ] Sì [ ] No
Eventuali dubbi sono stati sottoposti a DSGA/Dirigente/referente competente prima di procedere?	[ ] Sì [ ] No

Allegato. Scheda sintetica .

FARE	NON FARE
Usare strumenti autorizzati e rispettare la scheda di condizioni d'uso.	Usare strumenti personali o non approvati per attività scolastiche.
Scrivere prompt con dati fittizi, anonimi o generici.	Inserire nomi, classi, diagnosi, voti, note, foto, file riservati.
Controllare sempre fonti, dati, riferimenti e tono dell'output.	Copiare e incollare output senza verifica.
Dichiarare l'uso dell'IA quando richiesto nelle attività didattiche.	Presentare come interamente proprio un lavoro generato dall'IA se le regole lo vietano.
Segnalare subito errori, caricamenti accidentali o usi impropri.	Gestire da soli incidenti o cancellare tracce senza indicazioni.
Mantenere decisioni e responsabilità in capo alle persone.	Delegare all'IA valutazioni, provvedimenti o scelte su persone.

Formula breve da ricordare

AUTORIZZAZIONE - MINIMIZZAZIONE - VERIFICA - RESPONSABILITÀ. Se manca uno di questi quattro elementi, l'uso dell'IA non deve proseguire.