



Ministero dell'Istruzione e del Merito
ISTITUTO COMPRENSIVO ROSSANO 1

Scuole dell'Infanzia, Primarie e Secondarie a Indirizzo Musicale

Sede centrale e amministrativa: Via Martucci, 18 - 87064 - Corigliano-Rossano (CS)

Codice meccanografico: CSIC8AM004 - Codice fiscale: 97028290787 Tel. 0983/521143

Codice IPA: istsc_csic8am004 - Codice univoco di fatturazione: UF2MCT

e-mail: peo_csic8am004@istruzione.it - pec: csic8am004@pec.istruzione.it - Sito web: www.icrossano1.edu.it

Allegato al decreto Prot. n. vedasi segnature del 21/10/2026

LINEE GUIDA OPERATIVE

PER LA GESTIONE E LA CONDIVISIONE DEI DOCUMENTI RISERVATI E SENSIBILI DEGLI ALUNNI

Indicazioni per il personale docente e gli uffici di segreteria

1. Premessa e finalità

Ogni giorno la scuola tratta documenti che contengono informazioni personali e riservate degli alunni: Piani Educativi Individualizzati (PEI), Piani Didattici Personalizzati (PDP), certificazioni sanitarie, relazioni specialistiche, verbali dei Gruppi di Lavoro Operativo per l'inclusione (GLO) e altri documenti riguardanti situazioni personali, familiari o di salute, provvedimenti disciplinari e procedimenti individuali.

Una corretta gestione di questa documentazione è indispensabile per tutelare la riservatezza degli alunni e delle famiglie e, allo stesso tempo, per consentire ai docenti e al personale autorizzato di svolgere le proprie attività.

La condivisione dei documenti tramite il registro elettronico, le piattaforme cloud istituzionali e gli altri strumenti digitali adottati dalla scuola è consentita, a condizione che avvenga nel rispetto delle regole sulla protezione dei dati personali. In particolare, ogni documento deve essere accessibile esclusivamente a chi ha effettiva necessità di conoscerne il contenuto: un errore nella scelta dei destinatari può infatti comportare la divulgazione di informazioni riservate, anche quando si utilizzano piattaforme istituzionali protette da credenziali personali.

Con il provvedimento del 27 febbraio 2025 (doc. web n. 10126123) il Garante per la protezione dei dati personali ha esaminato il caso di una scuola primaria in cui una docente di sostegno, intendendo condividere il PEI di un alunno con la sola famiglia tramite il registro elettronico, aveva selezionato per errore anche l'intera classe: il documento è rimasto accessibile a tutti i genitori per circa 22 minuti e uno di essi ne ha diffuso uno screenshot nella chat di classe. Il Garante ha accertato una comunicazione illecita di dati personali, compresi dati relativi alla salute, precisando che l'uso di un'area riservata del registro non garantisce di per sé la liceità della condivisione e che l'involontarietà dell'errore e la sua rapida correzione non hanno eliminato la violazione.

Con un successivo provvedimento del 10 aprile 2025 (doc. web n. 10144156) il Garante ha inoltre ritenuto illecita la pubblicazione, nella bacheca del registro elettronico, di una convocazione del GLO che riportava in chiaro il nome di un'alunna, accessibile ai genitori dell'intera classe.

Questi episodi dimostrano che la presenza di un'area riservata, accessibile con credenziali personali o con CIE, non elimina il rischio di accessi non autorizzati quando la condivisione è impostata in modo errato: per questo è opportuno introdurre ulteriori livelli di protezione.

Per ridurre questi rischi, la scuola adotta le presenti Linee guida, predisposte dalla Dirigente scolastica con il supporto del DPO, che forniscono istruzioni pratiche per la conservazione, la consultazione e la condivisione dei documenti riservati.

Le indicazioni si fondano sui principi del Regolamento (UE) 2016/679, in particolare sugli artt. 5, 9, 25 e 32, e integrano le disposizioni contenute nei regolamenti e nelle istruzioni interne dell'Istituzione scolastica.

2. Documenti che richiedono particolare attenzione

Le presenti istruzioni si applicano principalmente ai documenti contenenti dati relativi alla salute, alla disabilità, ai disturbi dell'apprendimento e ad altre situazioni personali delicate. Rientrano in questa categoria:

- PEI e relativi allegati;
- PDP, soprattutto se contengono diagnosi o informazioni sanitarie;
- certificazioni mediche e diagnostiche;
- relazioni di psicologi, terapisti e altri specialisti;
- verbali GLO e documentazione relativa all'inclusione;
- relazioni su situazioni familiari o sociali particolarmente delicate;
- altri documenti contenenti dati personali per i quali sono necessarie specifiche cautele.

Non tutti questi documenti contengono necessariamente categorie particolari di dati ai sensi dell'art. 9 del GDPR; la scuola deve comunque adottare misure di protezione proporzionate alla natura delle informazioni e ai rischi derivanti dalla loro divulgazione.

Anche documenti privi di diagnosi possono rivelare indirettamente informazioni delicate: ad esempio, una convocazione del GLO che riporta il nominativo dell'alunno può far conoscere la sua condizione personale pur senza allegare alcun documento sanitario. Di seguito le cautele consigliate per le principali tipologie di documenti.

Tipologia di documento	Cautele consigliate
PEI e relativi allegati	Accesso strettamente selettivo; pseudonimizzazione e/o cifratura nelle condivisioni di file
PDP per DSA/BES	Stesse cautele, soprattutto in presenza di diagnosi o informazioni sanitarie
Diagnosi e certificazioni sanitarie, relazioni di psicologi e terapisti	Accesso molto ristretto, preferibilmente attraverso sistemi documentali dedicati
Verbali GLO, convocazioni individuali e documentazione di inclusione	Limitazione ai partecipanti legittimati e protezione dei contenuti; nessuna pubblicazione nominativa in bacheca

3. Regola generale: condividere soltanto con chi è autorizzato

Prima di condividere qualsiasi documento riservato, il personale deve verificare chi abbia effettivamente necessità di consultarlo.

L'accesso può essere consentito, nei limiti delle rispettive funzioni, ai docenti curricolari della classe, ai docenti di sostegno, alla Dirigente scolastica, al personale amministrativo competente e agli altri soggetti legittimati.

Non è corretto presumere che tutti i docenti dell'Istituto, tutti i componenti di un gruppo di lavoro o tutto il personale di segreteria possano accedere indistintamente alla documentazione degli alunni. Occorre inoltre distinguere i documenti necessari alla programmazione didattica dalle certificazioni sanitarie e dalle relazioni specialistiche, che possono richiedere autorizzazioni più ristrette.

Regola da rispettare: ogni documento deve essere condiviso soltanto con i destinatari effettivamente autorizzati e attraverso gli strumenti istituzionali individuati dalla scuola.

4. Utilizzo del registro elettronico

Il registro elettronico può essere utilizzato per condividere PEI, PDP e altri documenti riservati, purché disponga di una funzione che consenta di selezionare i singoli destinatari.

È importante distinguere la bacheca generale, la bacheca di classe e le funzioni di condivisione individuale, perché non sempre queste sezioni applicano gli stessi criteri di visibilità. Per i documenti riferiti al singolo alunno si utilizza esclusivamente la funzione di condivisione individuale.

Prima di caricare un documento, il docente deve:

1. accedere alla sezione del registro elettronico destinata alla condivisione individuale;
2. selezionare esclusivamente l'alunno o i destinatari interessati;
3. verificare che non risultino selezionate opzioni riferite all'intera classe, a tutti i genitori o ad altri gruppi;
4. controllare il nome del file, evitando riferimenti personali non necessari;
5. valutare l'utilizzo della pseudonimizzazione o di un file protetto con password, secondo le indicazioni fornite;
6. controllare nuovamente i destinatari prima di confermare l'operazione.

Le bacheche generali non devono essere utilizzate per pubblicare PEI, PDP, convocazioni individuali del GLO o altri documenti dai quali sia possibile ricavare informazioni riservate su uno specifico alunno. Anche la presenza di una password sul file non autorizza a condividerlo indiscriminatamente.

La cifratura del file è una misura aggiuntiva particolarmente utile quando il sistema non permette di verificare agevolmente l'effettiva visibilità del documento o quando esiste il rischio di selezionare accidentalmente destinatari ulteriori; negli altri casi la pseudonimizzazione può già rappresentare un'adeguata misura di minimizzazione.

Esempio: condivisione di un PEI con la famiglia

Il docente accede alla sezione del registro elettronico dedicata alla condivisione individuale, seleziona esclusivamente l'alunno interessato e verifica che il documento non sia accessibile agli altri genitori. Se la

scuola ha previsto la cifratura come ulteriore misura anche nella condivisione con la famiglia, il docente carica il file protetto con password e comunica la password ai genitori attraverso un canale distinto. In questo modo un'eventuale selezione errata dei destinatari non consentirebbe automaticamente la lettura del contenuto, purché la password non sia accessibile a soggetti non autorizzati. Resta comunque necessario verificare che il titolo del documento, il messaggio di accompagnamento o l'avviso del registro non rendano identificabile l'alunno.

5. Utilizzo delle piattaforme cloud istituzionali

La scuola può utilizzare ambienti cloud istituzionali o altre piattaforme autorizzate, per conservare e condividere la documentazione.

I documenti devono essere collocati in cartelle riservate, accessibili soltanto al personale che ne ha necessità. In particolare, occorre:

- utilizzare esclusivamente account istituzionali;
- evitare cartelle accessibili a tutto il personale scolastico;
- non utilizzare collegamenti pubblici o accessibili a chiunque possieda il link;
- attribuire i permessi di consultazione o modifica secondo le effettive esigenze;
- non trasferire documenti riservati su cloud personali;
- segnalare al personale incaricato della gestione della piattaforma eventuali autorizzazioni non corrette;
- attivare l'autenticazione multifattore, ove disponibile;
- limitare la possibilità di download quando non necessaria e quando la piattaforma lo consente;
- attivare il tracciamento degli accessi (log) e conservarlo secondo le regole applicabili.

I permessi devono essere aggiornati quando cambiano i docenti, le classi, gli incarichi o le necessità di accesso e verificati periodicamente, in particolare in occasione di cambi di classe, trasferimenti di alunni, sostituzioni di docenti e cessazioni dal servizio.

La scuola può prevedere cartelle riservate ai consigli di classe o ai gruppi di docenti autorizzati, mantenendo separata la documentazione sanitaria, che richiede una consultazione più limitata.

Una cartella dedicata alla documentazione inclusiva di una classe non deve contenere indiscriminatamente ogni certificazione sanitaria o ogni documento del fascicolo personale: per questi ultimi possono essere predisposti spazi separati con autorizzazioni ulteriormente ristrette, oppure può essere prevista la consultazione diretta in segreteria, evitando la condivisione digitale quando non strettamente necessaria.

Esempio: condivisione di PEI e PDP tra docenti

L'amministratore del sistema configura la cartella cloud istituzionale della classe in modo che sia accessibile soltanto ai docenti autorizzati. I documenti possono essere gestiti come copie operative pseudonimizzate, quando la finalità consente di evitare l'identificazione diretta, valutando se applicare un'ulteriore cifratura in base alla sicurezza già garantita dalla piattaforma e alle esigenze di consultazione e aggiornamento. Non è consentito distribuire copie dei PEI attraverso chat informali, account personali o cartelle condivise con tutti i docenti dell'Istituto.

6. Pseudonimizzazione dei documenti

La pseudonimizzazione è una misura che riduce la possibilità di identificare direttamente l'alunno, sostituendone i dati identificativi con un codice.

Quando è compatibile con la finalità della condivisione – ad esempio per la consultazione e la verifica del PEI da parte dei docenti della classe – è possibile utilizzare il codice identificativo dell'alunno presente nel sistema SIDI oppure un diverso codice interno predisposto dalla scuola. Ad esempio:

<i>Anziché denominare il file</i>	<i>si può utilizzare</i>
PEI_Mario_Rossi_2026.docx	PEI_A01234_2026.docx

Questa modalità evita che il nome del file riporti direttamente il nominativo dell'alunno, ma da sola non costituisce una pseudonimizzazione completa: è necessario verificare anche il contenuto, eliminando o sostituendo gli elementi identificativi non necessari alla specifica condivisione. La scuola deve inoltre conservare separatamente e in modo sicuro le informazioni che consentono di associare il codice all'alunno.

Il codice SIDI non è anonimo: poiché la scuola dispone delle informazioni per ricondurlo allo studente, il documento resta un dato personale pseudonimizzato e il codice stesso è un riferimento da proteggere. La pseudonimizzazione, inoltre, non elimina il rischio se il documento contiene riferimenti alla classe, ai docenti, alla famiglia o ad altre circostanze che consentono l'identificazione indiretta.

Come procedere con Microsoft Word

1. Aprire il documento originale.
2. Crearne una copia mediante la funzione «Salva con nome».
3. Sostituire nome e cognome dell'alunno con il codice identificativo.
4. Sostituire il nominativo anche nel testo e verificare che non siano presenti altri elementi che permettano un'identificazione diretta o indiretta non necessaria.
5. Controllare commenti, revisioni, intestazioni e proprietà del documento.
6. Salvare la copia e condividerla nella cartella istituzionale autorizzata.

Attenzione: i PEI e i PDP ufficiali devono mantenere tutti gli elementi identificativi e formali necessari. La pseudonimizzazione va quindi utilizzata per eventuali copie operative, senza alterare il documento originale che confluirà nel fascicolo.

7. Cifratura dei documenti mediante password

La cifratura protegge il contenuto di un documento, impedendone la lettura a chi non dispone della password necessaria per aprirlo.

È una misura particolarmente utile quando un PEI, un PDP o un altro documento riservato deve essere trasmesso come file autonomo oppure condiviso in un ambiente nel quale esiste il rischio di selezionare destinatari errati. La password deve proteggere l'apertura del file e non soltanto impedirne la modifica.

La password che limita soltanto la modifica non impedisce di leggere il contenuto e non è quindi sufficiente a tutelare la riservatezza di un PEI o di un PDP. Occorre inoltre ricordare che la cifratura impedisce la lettura del contenuto, ma non nasconde l'esistenza del documento né la sua associazione all'alunno, se questi elementi emergono dal nome del file, dall'avviso del registro elettronico o dal messaggio di accompagnamento: cifratura e pseudonimizzazione riducono il rischio, ma non sostituiscono la verifica dei destinatari e di tutti gli elementi della comunicazione.

Come proteggere un documento Word

Utilizzando Microsoft Word nella versione desktop per Windows, occorre:

1. aprire il documento;
2. selezionare File;
3. accedere alla sezione Informazioni;
4. fare clic su Proteggi documento;
5. selezionare Crittografia con password;
6. inserire una password e confermarla;
7. salvare il documento.

Percorso: File > Informazioni > Proteggi documento > Crittografia con password

Dopo aver salvato il file, è necessario chiuderlo e riaprirlo per verificare che Word richieda effettivamente la password prima di mostrarne il contenuto. La password va comunicata ai destinatari separatamente; si consiglia tuttavia di definire a inizio anno una password per ciascuna classe (gruppo docenti), da utilizzare per la condivisione e la consultazione dei documenti sensibili.

Per rimuovere la password quando non è più necessaria, si segue lo stesso percorso, si cancella la password inserita e si salva il documento.

Come proteggere un documento PDF

Microsoft Word consente di salvare un documento in formato PDF, ma la semplice conversione non garantisce la cifratura del file, e la password eventualmente applicata al documento Word non viene necessariamente estesa anche al PDF.

Se non è disponibile una soluzione idonea alla cifratura del PDF, è preferibile condividere il documento Word già cifrato, quando il formato è compatibile con le esigenze del destinatario. Non devono essere utilizzati siti Internet o servizi online per proteggere documenti contenenti dati sensibili.

Come gestire correttamente le password

La password deve essere robusta e non facilmente individuabile: non devono essere utilizzati il nome dell'alunno, la data di nascita, il codice fiscale, il nome della scuola o altre informazioni prevedibili.

La password deve essere comunicata esclusivamente ai destinatari autorizzati, preferibilmente attraverso un canale diverso da quello utilizzato per trasmettere il documento. Ad esempio, il file può essere condiviso nell'area specifica del registro elettronico o in una cartella cloud istituzionale, mentre la password può essere comunicata attraverso un altro canale oppure definita a inizio anno per ciascun gruppo docenti di classe.

Non è opportuno utilizzare una password unica e permanente per tutti i PEI o PDP dell'Istituto.

La cifratura può complicare la collaborazione simultanea sui documenti e la ricerca nei contenuti. Per le condivisioni interne in ambienti cloud correttamente configurati, la scuola può quindi privilegiare la pseudonimizzazione delle copie operative, le autorizzazioni individuali, l'autenticazione sicura e il tracciamento degli accessi, senza imporre necessariamente una password aggiuntiva a ogni documento; la cifratura va invece privilegiata per le trasmissioni più a rischio, in particolare quando il documento contiene informazioni sanitarie e viene trasferito come file autonomo.

8. Quale misura utilizzare nelle diverse situazioni

La scelta delle misure dipende dalla tipologia del documento, dai destinatari e dalle caratteristiche dello strumento utilizzato.

Situazione	Modalità operativa consigliata
PEI da condividere con la famiglia	Area individuale del registro elettronico, controllo dei destinatari e cifratura aggiuntiva se prevista
Copia operativa di PEI/PDP da consultare tra docenti autorizzati	Cartella cloud istituzionale, pseudonimizzazione e accesso selettivo
Documento sanitario trasmesso come allegato (se strettamente necessario)	Cifratura con password di apertura e invio sicuro e separato della password
Archivio cloud contenente più PEI	Cartelle e permessi differenziati, con ulteriori protezioni per i file più delicati
Documento condiviso temporaneamente con un soggetto esterno legittimato (es. rappresentante UMV)	Verifica della legittimazione, minimizzazione/pseudonimizzazione e canale sicuro
Documentazione integrale conservata nel fascicolo dell'alunno	Archivio istituzionale con accessi limitati al personale competente

La pseudonimizzazione e la cifratura possono essere utilizzate insieme, ma non è necessario applicarle automaticamente a ogni documento: la prima misura da garantire resta sempre la corretta selezione dei destinatari.

9. Comportamenti da evitare

Per prevenire errori e divulgazioni accidentali, il personale deve evitare di:

- ✗ caricare PEI, PDP o documenti riservati nelle bacheche generali o di classe;
- ✗ condividere documenti attraverso cartelle accessibili indistintamente a tutto il personale;
- ✗ utilizzare account personali di posta elettronica o di cloud;
- ✗ inviare documenti contenenti dati sanitari tramite chat informali o gruppi di messaggistica;
- ✗ inserire nomi, diagnosi o altre informazioni riservate nei titoli dei file, quando non necessario;
- ✗ condividere file protetti e relative password nello stesso messaggio;
- ✗ utilizzare siti non autorizzati per convertire, modificare o proteggere documenti;
- ✗ lasciare documenti riservati accessibili su postazioni condivise;

X inviare documenti senza aver verificato la legittimazione dei destinatari.

10. Cosa fare in caso di condivisione errata

Se un documento riservato viene condiviso per errore con destinatari non autorizzati, occorre intervenire immediatamente. Il docente o l'operatore che rileva l'errore deve:

1. interrompere la condivisione o revocare le autorizzazioni errate;
2. informare tempestivamente la Dirigente scolastica o il referente interno individuato per la gestione degli incidenti, senza attendere eventuali segnalazioni delle famiglie;
3. indicare quale documento è stato coinvolto, a chi risultava accessibile e per quanto tempo;
4. collaborare alle verifiche richieste dalla scuola.

La Dirigente scolastica, con il supporto del DPO, ricostruisce l'accaduto e valuta se l'evento costituisca una violazione di dati personali ai sensi dell'art. 4, punto 12, del GDPR, verificando quali informazioni fossero accessibili, per quanto tempo, a quali soggetti e se risultino accessi, download o ulteriori comunicazioni (ad esempio screenshot diffusi in chat).

Se la violazione presenta un rischio per i diritti e le libertà delle persone, l'art. 33 del GDPR prevede la notifica al Garante, ove possibile entro 72 ore dal momento in cui la scuola ne è venuta a conoscenza; in presenza di un rischio elevato, l'art. 34 richiede anche la comunicazione agli interessati. L'incidente e la valutazione effettuata sono comunque documentati, anche quando si ritiene che non sussistano i presupposti per la notifica.

La pseudonimizzazione o la presenza di una password sul file possono ridurre le conseguenze dell'errore, ma non escludono automaticamente la violazione, soprattutto quando restano comunque accessibili informazioni che consentono di identificare l'alunno.

La cifratura è comunque un elemento rilevante nella valutazione del rischio: se il documento era cifrato efficacemente e la password non è stata compromessa, la possibilità che i destinatari non autorizzati ne abbiano letto il contenuto risulta significativamente ridotta.

11. Verifica finale prima della condivisione

Prima di confermare la condivisione di un PEI, di un PDP o di un altro documento riservato, il personale effettua un ultimo controllo:

- ☐ Sto utilizzando un ambiente istituzionale autorizzato?
- ☐ Ho selezionato esclusivamente i destinatari legittimati?
- ☐ Ho verificato che il documento non sia visibile all'intera classe?
- ☐ Il titolo del file evita riferimenti personali non necessari?
- ☐ Ho valutato la pseudonimizzazione o la cifratura del file?
- ☐ Se uso una password, la comunico tramite un canale distinto o è già nota ai destinatari?
- ☐ Ho verificato l'effettiva visibilità del documento?

Questi controlli consentono di ridurre al minimo gli incidenti e i rischi di diffusione dei dati.

12. Disposizioni organizzative e responsabilità

La Dirigente scolastica assicura l'attuazione delle presenti Linee guida e individua gli strumenti istituzionali autorizzati per la gestione e la condivisione dei documenti riservati (ad es. registro elettronico, spazio cloud ad accesso riservato). Il personale docente e amministrativo è tenuto a rispettare le istruzioni ricevute, utilizzando esclusivamente gli strumenti e le modalità previsti dalla scuola.

Gli amministratori delle piattaforme digitali curano, secondo gli incarichi attribuiti, la configurazione degli accessi, l'aggiornamento delle autorizzazioni e il supporto tecnico al personale.

Gli amministratori verificano inoltre che le piattaforme in uso dispongano di funzioni che consentano ai docenti di controllare i destinatari e l'ambito di visibilità prima di confermare la condivisione.

Eventuali difficoltà operative, limitazioni tecniche delle piattaforme o dubbi sulla corretta modalità di condivisione devono essere segnalati alla Dirigente scolastica o al referente individuato prima di procedere alla trasmissione dei documenti.

Le presenti Linee guida integrano le istruzioni già impartite al personale autorizzato al trattamento dei dati e le disposizioni contenute nei regolamenti interni relativi al registro elettronico, alla gestione documentale e all'utilizzo delle piattaforme digitali. La loro applicazione costituisce una misura organizzativa finalizzata a prevenire accessi non autorizzati e divulgazioni accidentali, garantendo al tempo stesso la corretta gestione della documentazione necessaria alle attività didattiche e amministrative.

LA DIRIGENTE SCOLASTICA

Anna Maria VECCHIO

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