Istituto Comprensivo "C. Simonetta" Via G. Dardani, 20 – 88833 Caccuri (KR)
Cod. Fisc. 91021260798 - E-Mail: kric821002@istruzione.it

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

Documento predisposto dal Dirigente scolastico
con il supporto del Responsabile della Protezione dei Dati (DPO)

1. Premessa e finalità

La scuola gestisce quotidianamente documenti che contengono informazioni personali e riservate degli alunni: tra questi rientrano i Piani Educativi Individualizzati (PEI), i Piani Didattici Personalizzati (PDP), le certificazioni sanitarie, le relazioni specialistiche, i verbali dei Gruppi di Lavoro Operativo per l'inclusione (GLO) e altri documenti relativi a situazioni personali, familiari o di salute, provvedimenti disciplinari e procedimenti individuali.
La **corretta gestione** di questa documentazione è necessaria per **tutelare la riservatezza degli studenti** e delle famiglie e, nello stesso tempo, consentire ai docenti e al personale autorizzato di svolgere le proprie attività.

La condivisione dei documenti attraverso il registro elettronico, le piattaforme cloud istituzionali e gli altri strumenti digitali adottati dalla scuola è consentita, purché avvenga nel rispetto delle regole sulla protezione dei dati personali. In particolare, occorre garantire che ogni documento sia accessibile esclusivamente alle persone che hanno effettiva necessità di conoscerne il contenuto, perché un errore nella selezione dei destinatari può comportare la divulgazione di informazioni riservate, anche quando si utilizzano piattaforme istituzionali protette da credenziali personali.

Il Garante per la protezione dei dati personali è intervenuto su un caso nel quale un PEI, destinato alla famiglia di un alunno, era stato erroneamente condiviso attraverso il registro elettronico con tutti i genitori della classe.. L'episodio dimostra che la presenza di un'area riservata non elimina il rischio di accessi non autorizzati quando la condivisione viene configurata in maniera errata.
Per ridurre questi rischi, la scuola adotta le presenti Linee guida, predisposte dal Dirigente scolastico 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 articoli 5, 9, 25 e 32, e integrano le disposizioni contenute nei regolamenti e nelle istruzioni interne dell'Istituzione scolastica.

2. Quali documenti richiedono particolare attenzione

Le presenti istruzioni si applicano principalmente ai **documenti che contengono 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 quando contengono diagnosi o informazioni sanitarie;
- certificazioni mediche e diagnostiche;
- relazioni di psicologi, terapisti e altri specialisti;
- verbali GLO e documentazione relativa all'inclusione;
- relazioni riguardanti situazioni familiari o sociali particolarmente delicate;
- ulteriori documenti che contengono dati personali per i quali occorrono specifiche cautele.

Istituto Comprensivo "C. Simonetta" Via G. Dardani, 20 – 88833 Caccuri (KR)
Cod. Fisc. 91021260798 - E-Mail: kric821002@istruzione.it

Non tutti questi documenti contengono necessariamente categorie particolari di dati ai sensi dell'articolo 9 del GDPR. Tuttavia, la scuola deve adottare misure di protezione proporzionate alla natura delle informazioni e ai rischi della loro divulgazione.

3. Regola generale: condividere soltanto con chi è autorizzato

Prima di condividere qualsiasi documento riservato, il personale deve verificare **chi ha effettivamente necessità di consultarlo**.
L'accesso può essere consentito ai docenti curricolari della classe, ai docenti di sostegno, al Dirigente scolastico, al personale amministrativo competente e agli altri soggetti legittimati, nei limiti delle rispettive funzioni.
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.
La regola da rispettare è che 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**.
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.
6. Controllare nuovamente i destinatari prima di confermare l'operazione.

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

5. Utilizzo delle piattaforme cloud istituzionali

La scuola può utilizzare ambienti cloud istituzionali, come Microsoft 365, Google Workspace for Education 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:

- 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;

Istituto Comprensivo "C. Simonetta" Via G. Dardani, 20 – 88833 Caccuri (KR)
Cod. Fisc. 91021260798 - E-Mail: kric821002@istruzione.it

- segnalare al personale incaricato della gestione della piattaforma eventuali autorizzazioni non corrette.

I permessi devono essere aggiornati quando cambiano i docenti, le classi, gli incarichi o le necessità di accesso.
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.

6. Pseudonimizzazione dei documenti

La pseudonimizzazione è una misura che permette di **ridurre l'identificazione diretta dell'alunno attraverso la sostituzione dei suoi dati identificativi con un codice**.
Quando risulta compatibile con la finalità della condivisione, ad esempio per la consultazione e 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, anziché denominare un documento: PEI_Mario_Rossi_2026.docx
si può utilizzare: PEI_A01234_2026.docx

Questa modalità evita che il nome del file riporti direttamente il nominativo dell'alunno, ma non costituisce, da sola, 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.

- **Come procedere con Microsoft Word**
  1. Aprire il documento originale.
  2. Creare una copia mediante la funzione Salva con nome.
  3. Sostituire il nome e il cognome dell'alunno con il codice identificativo.
  4. Sostituire anche nel testo il nominativo 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.

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

7. Cifratura dei documenti mediante password

La cifratura permette di proteggere il contenuto di un documento **impedendone la lettura a chi non dispone della password necessaria per aprirlo**.
Si tratta di una misura particolarmente utile quando un PEI,, un PDP o altro documento riservato deve essere trasmesso come file autonomo oppure condiviso in un ambiente nel quale sussiste il rischio di selezionare destinatari errati. La password deve proteggere l'apertura del file e non soltanto impedirne la modifica.

- **Come proteggere un documento Word**

Utilizzando Microsoft Word nella versione desktop per Windows, occorre:

1. Aprire il documento.
2. Selezionare *File*.

Istituto Comprensivo "C. Simonetta" Via G. Dardani, 20 – 88833 Caccuri (KR)
Cod. Fisc. 91021260798 - E-Mail: kric821002@istruzione.it

3. Accedere alla sezione *Informazioni*.
4. Fare clic su *Proteggi documento*.
5. Selezionare *Crittografa con password*.
6. Inserire una password e confermarla.
7. Salvare il documento.

Il percorso operativo è:
File > Informazioni > Proteggi documento > Crittografa 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 deve essere comunicata ai destinatari separatamente, ma si consiglia di definire ad inizio anno una password per ciascuna classe (gruppo docenti) da utilizzare per la condivisione e consultazione dei documenti sensibili.

- **Come proteggere un documento PDF**

Microsoft Word permette 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 è detto che venga automaticamente applicata 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 risulta compatibile con le esigenze del destinatario, e **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 su una cartella cloud istituzionale e la password può essere comunicata attraverso un diverso canale o definita ad inizio anno per ciascun gruppo docenti classe.
Non è opportuno utilizzare una password unica e permanente per tutti i PEI o PDP dell'istituto.

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 RE, controllo dei destinatari e cifratura aggiuntiva se prevista
Copia PEI/PDP operativa 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

Istituto Comprensivo "C. Simonetta" Via G. Dardani, 20 – 88833 Caccuri (KR)
Cod. Fisc. 91021260798 - E-Mail: kric821002@istruzione.it

Documento condiviso temporaneamente con un soggetto esterno legittimato (es. rappresentante UMV)	Verifica della legittimazione, minimizzazione/pseudonomizzazione 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 rimane 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 di posta elettronica o cloud personali;
- inviare documenti contenenti dati sanitari attraverso 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;
- inviare documenti senza aver verificato la legittimità dei destinatari.

10. Cosa fare in caso di condivisione errata

Se un documento riservato viene condiviso accidentalmente 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 il Dirigente scolastico o il referente interno individuato per la gestione degli incidenti.
3. Indicare quale documento è stato coinvolto, a chi risultava accessibile e per quanto tempo.
4. Collaborare alle verifiche richieste dalla scuola.

Il Dirigente scolastico, con il supporto del DPO, valuterà l'evento secondo gli articoli 33 e 34 del GDPR, verificando se costituisce una violazione di dati personali e se ricorrono gli obblighi di notifica al Garante o di comunicazione agli interessati.
La presenza della pseudonomizzazione o di una password sul file può ridurre le conseguenze dell'errore, ma non esclude automaticamente la violazione, soprattutto quando risultano comunque accessibili informazioni che permettono di identificare l'alunno.

11. Verifica finale prima della condivisione

Prima di confermare la condivisione di un PEI, PDP o altro documento riservato, il personale deve effettuare 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 con un canale distinto o è già nota ai destinatari?
- Ho verificato l'effettiva visibilità del documento?

Istituto Comprensivo "C. Simonetta" Via G. Dardani, 20 – 88833 Caccuri (KR)
Cod. Fisc. 91021260798 - E-Mail: kric821002@istruzione.it

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

12. Disposizioni organizzative e responsabilità

Il Dirigente scolastico assicura l'attuazione delle presenti Linee guida e individua gli strumenti istituzionali autorizzati per la gestione e la condivisione dei documenti riservati (es. RE, spazio cloud ad accesso riservato) e il personale docente e amministrativo è tenuto a rispettare le istruzioni ricevute, utilizzando esclusivamente gli strumenti e le modalità previste 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.
Eventuali difficoltà operative,, limitazioni tecniche delle piattaforme o dubbi sulla corretta modalità di condivisione devono essere segnalati al Dirigente scolastico 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.

Il presente documento è stato predisposto con il supporto e la consulenza del Responsabile della Protezione dei Dati (DPO) dott.ssa Anna CIMA.

F.to/ Il Dirigente scolastico
Dott.ssa Rosa Audia