

**Vargiu Scuola Srl**

Via dei Tulipani 7/9 – Assemini (CA) - 09032

Sito: vargiuscuola.itcommerciale@vargiuscuola.it

tel: 070271526, 070271560

partita iva: 03679880926

Alle scuole che ci hanno affidato l'incarico di RPD
o a cui forniamo servizi di consulenza normativa

VS_DPO 107/2026

Assemini, 3/10/2026

Riservatezza dei documenti e delle comunicazioni sui dati particolari degli alunni: strumenti di condivisione e tecniche di cifratura

Con la [nota DPO 104/2026](#) abbiamo fornito alle scuole le indicazioni per l'avvio dell'anno scolastico sull'uso del Registro Elettronico, soffermandoci sulle aree riservate e sulla condivisione dei documenti contenenti dati particolari degli alunni, e abbiamo proposto a questo scopo due tecniche indicate espressamente dall'art. 32 del GDPR: la **pseudonimizzazione** e la **cifratura**. Le numerose richieste di chiarimento che ci sono pervenute nei giorni successivi ci hanno convinto dell'opportunità di tornare sull'argomento con una nota di taglio più pratico, estendendo il discorso dal Registro Elettronico a tutti gli strumenti con i quali documenti e informazioni riservate circolano nella scuola: le chiavette USB, i computer della scuola e quelli personali dei docenti, la posta elettronica, le piattaforme come Google Classroom.

Le considerazioni che seguono nascono dalla nostra esperienza quotidiana. Vargiu Scuola svolge il ruolo di Responsabile della Protezione dei Dati per un numero molto ampio di istituti scolastici e, in altre scuole, quello di amministratore dei sistemi informatici. Si tratta di ruoli che non assumiamo mai contemporaneamente nel medesimo istituto, in ragione del conflitto di interessi che si determinerebbe fra chi gestisce i sistemi e chi è chiamato a vigilare sulla correttezza dei trattamenti; ma proprio l'esercizio di entrambe le funzioni ci consente di osservare il fenomeno delle violazioni di dati da due prospettive complementari: quella di chi ne raccoglie la segnalazione e ne valuta le conseguenze, e quella di chi interviene sui dispositivi e sulle piattaforme.

1. Gli incidenti che osserviamo più di frequente

Il primo dato che la nostra esperienza restituisce è la frequenza, ben superiore a quanto comunemente si immagina, di violazioni di dati personali causate da sottrazione o perdita di supporti fisici di archiviazione o furti di computer e di notebook. Ci vengono segnalati con regolarità furti avvenuti nei locali scolastici, nelle segreterie, nelle aule e nei laboratori, spesso in occasione di intrusioni notturne o durante i periodi di chiusura, e furti che coinvolgono i dispositivi personali dei docenti: il notebook sottratto dall'auto o dall'abitazione, la borsa dimenticata sul treno, la **chiavetta USB** smarrita nel tragitto fra la scuola e casa. In tutti questi casi, se sul dispositivo si trovano PEI, PDP, relazioni, verbali o comunicazioni relative agli alunni, e se questi documenti sono conservati in chiaro, alla perdita materiale del bene si aggiunge una violazione di dati personali che la scuola deve valutare, annotare e, nella maggior parte dei casi, notificare al Garante.

Il secondo fenomeno, già descritto nella [nota DPO 104/2026](#), è quello degli **errori di caricamento** sul Registro Elettronico o sulle piattaforme di Google o Microsoft: il documento riservato inserito nell'area sbagliata, o reso visibile all'intera classe per un segno di spunta di troppo. Sono incidenti gravi, perché in pochi minuti l'intera comunità dei genitori, o degli alunni, viene a conoscenza di informazioni delicate e riservate su un compagno: una diagnosi, una situazione familiare difficile, un percorso di sostegno. Le conseguenze per l'alunno interessato e per la sua famiglia possono essere

pesanti e difficilmente rimediabili, perché ciò che è stato letto non può essere “cancellato”, e il danno alla relazione fra la famiglia e la scuola è spesso profondo.

Il terzo fenomeno riguarda la **posta elettronica**. L’invio di un messaggio al destinatario sbagliato è forse l’errore più banale che si possa commettere, favorito dal completamento automatico degli indirizzi e dall’uso di liste di distribuzione dai nomi simili; ma per certe comunicazioni le sue conseguenze possono essere gravissime, perché il messaggio, una volta inviato, sfugge a ogni controllo della scuola e non può più essere ritirato.

Un caso che ci è stato sottoposto di recente lo dimostra con particolare evidenza. Un docente, convinto di scrivere alla lista di distribuzione dei colleghi del consiglio di classe, ha inviato un resoconto del colloquio appena avuto con i genitori di un alunno: un testo scritto di getto, franco e senza filtri, con valutazioni personali assai crude sull’alunno e sulla famiglia, pensate per restare nella cerchia ristretta dei colleghi. Il messaggio ha invece raggiunto le caselle di posta di tutti i genitori della classe. È facile immaginare le conseguenze: la violazione della riservatezza dell’alunno e della sua famiglia, l’esposizione del docente e dell’istituto, un conflitto con la famiglia che nessuna scusa successiva ha potuto ricomporre, oltre naturalmente agli adempimenti connessi alla gestione della violazione.

Il caso insegna che la cautela non riguarda soltanto i documenti “formali” come PEI e PDP. Anche un resoconto informale, una nota di lavoro o un messaggio fra colleghi possono contenere informazioni riservate, e vanno trattati con le stesse attenzioni.

2. L’esigenza di condividere le informazioni nel consiglio di classe

Tutto ciò non deve indurre a concludere che documenti e informazioni riservate non debbano circolare. Il consiglio di classe è un organo collegiale che, per svolgere la propria funzione educativa e valutativa, ha bisogno che tutti i suoi componenti conoscano le informazioni necessarie sugli alunni: il docente di sostegno, i docenti curricolari, il coordinatore devono poter consultare il PEI o il PDP, le relazioni e le osservazioni dei colleghi, e devono poterlo fare con tempestività nella preparazione delle attività e delle verifiche. Ne abbiamo parlato diffusamente nella [nota DPO 98/2025](#).

In alcuni contesti, e per documenti particolarmente riservati, il titolare del trattamento può legittimamente decidere che l’accesso avvenga soltanto mediante **presa visione dei documenti cartacei custoditi in segreteria**: una procedura che offre il massimo livello di riservatezza e che resta una scelta del tutto ragionevole. Non sempre, però, questa modalità è compatibile con le esigenze organizzative e didattiche. La presa visione in segreteria presuppone la presenza fisica del docente negli orari di apertura degli uffici, mal si concilia con l’organizzazione di istituti articolati su più plessi e con i docenti in servizio su più scuole, e rischia, paradossalmente, di spingere i docenti a fotografare i documenti o a farsene copie, spostandone la circolazione su canali ancora meno controllati.

La presa visione cartacea è dunque una facoltà del titolare, non un obbligo: la condivisione dei documenti in formato digitale sulle piattaforme istituzionali, fra i soli soggetti autorizzati, è pienamente lecita, come abbiamo chiarito nella nota 104/2026 anche alla luce del provvedimento del Garante del 27 febbraio 2025, a condizione che la scuola scelga strumenti adeguati e li accompagni con misure tecniche e organizzative idonee a contenere il rischio legato all’errore umano (artt. 5, par. 1, lett. f), e 32 del GDPR).

3. Gli strumenti di condivisione a confronto

Ogni scuola dovrà quindi valutare quali strumenti consentire, e a quali condizioni, per la condivisione di documenti e informazioni riservate. Gli strumenti in concreto utilizzati sono sostanzialmente tre.

Il primo è lo **scambio mediante dispositivi di memorizzazione**, in primo luogo le chiavette USB, e più in generale la conservazione dei documenti sui dispositivi personali dei docenti. Con la diffusione delle piattaforme cloud istituzionali, come Google Workspace e Microsoft 365, l’uso delle chiavette

per i documenti riservati si è progressivamente ridotto. Non è però scomparso. Le chiavette restano in uso nelle aule, per trasferire materiali sul computer collegato alla lavagna interattiva o al monitor, nel passaggio fra il lavoro svolto a casa sul computer personale e quello svolto a scuola, e talvolta nelle segreterie, per copie di lavoro o di sicurezza. È proprio la familiarità di questi usi quotidiani a far sottovalutare il rischio. La stessa chiavetta che contiene le presentazioni per la lezione finisce spesso per ospitare anche un PEI, una relazione o un verbale, conservati in chiaro e dimenticati. Si tratta di uno strumento del tutto fuori dal controllo della scuola: la chiavetta si smarrisce facilmente, passa di mano in mano e viene utilizzata anche per scopi personali, mentre le copie dei documenti si moltiplicano sui computer di casa senza che nessuno ne tenga traccia. Il rischio tipico è quello dello smarrimento o del furto, e quando si verifica la scuola non ha alcun modo di rimediare.

Il secondo è lo **scambio mediante posta elettronica**. È lo strumento più diffuso e più familiare, ma presenta due criticità. La prima è l'errore sul destinatario, di cui si è detto; la seconda è la moltiplicazione delle copie: ogni documento inviato per posta elettronica resta nelle caselle del mittente e di ciascun destinatario, può essere inoltrato, scaricato su dispositivi personali, conservato per anni, senza che la scuola possa più intervenire. Un messaggio inviato per errore non può essere ritirato. Ove si utilizzi la posta elettronica, deve trattarsi in ogni caso degli account istituzionali forniti dalla scuola e mai di caselle personali.

Il terzo è la **condivisione su piattaforme telematiche** gestite dalla scuola, come il Registro Elettronico o Google Classroom e gli spazi condivisi di Google Workspace o Microsoft 365. Il documento resta in un unico luogo, accessibile ai soli utenti autorizzati, con accessi tracciati; la scuola ne mantiene il controllo, può modificarne la visibilità e rimuoverlo, e non è necessario che ne circolino copie. Anche qui il rischio tipico è l'errore umano, nella scelta dell'area o dei destinatari, ma un errore che può essere individuato e corretto, riducendo il tempo di esposizione.

Strumento	Rischio principale	Controllo della scuola	Possibilità di rimediare all'errore
Chiavette USB e dispositivi personali	Smarrimento e furto; moltiplicazione incontrollata delle copie	Nessuno	Nessuna: il dispositivo sottratto non è recuperabile
Posta elettronica	Destinatario errato; inoltri e copie nelle caselle dei destinatari	Limitato agli account istituzionali	Nessuna, una volta inviato il messaggio
Piattaforme (Registro Elettronico, Classroom, spazi condivisi)	Scelta errata dell'area o dei destinatari	Pieno: accessi autorizzati e tracciati	Il documento può essere rimosso o la visibilità corretta

Tabella 1 – Confronto fra gli strumenti di condivisione di documenti e informazioni riservate.

Fra i tre strumenti è senz'altro da preferire il terzo, secondo le indicazioni già fornite nella nota DPO 104/2026, alla quale rinviamo per la configurazione delle aree riservate del Registro. Nessuno strumento, tuttavia, è esente dal rischio di errore, e in concreto la scuola non potrà escludere del tutto l'uso della posta elettronica o dei dispositivi di memorizzazione. Qualunque sia lo strumento utilizzato, occorre quindi adottare tecniche che riducano la probabilità che si verifichi una violazione (**minimizzazione dei rischi**) e che, se la violazione si verifica, ne limitino le conseguenze per gli interessati (**contenimento delle conseguenze**).

4. La pseudonimizzazione

La prima tecnica, già illustrata nella [nota 104/2026](#), è la **pseudonimizzazione**, che l'art. 4, n. 5, del GDPR definisce come il trattamento dei dati personali in modo tale che essi non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni siano conservate separatamente e soggette a misure tecniche e organizzative che ne garantiscano la riservatezza.

In termini pratici, significa sostituire nei documenti riservati il nome dell'alunno con un codice. All'inizio dell'anno scolastico la segreteria attribuisce a ciascun alunno interessato un codice alfanumerico, che non deve essere ricavabile dal nome, dalla data di nascita, dal numero di registro o da altre informazioni note, e riporta la corrispondenza fra codici e alunni in una tabella conservata in forma riservata e accessibile al solo personale autorizzato. Il codice viene comunicato ai docenti della classe, che redigono i documenti riservati (PEI, PDP, relazioni, osservazioni) riportando soltanto il codice e omettendo nome, codice fiscale, data di nascita, indirizzo e ogni altro dato identificativo. Se il documento giunge a terzi non autorizzati, questi non sono in grado di attribuirlo direttamente a un alunno specifico.

La tecnica presenta però due limiti. Il primo, già segnalato nella nota 104/2026, è che in un contesto ristretto come quello di una classe il contenuto del documento può rendere l'alunno riconoscibile anche in assenza del nome: i dati pseudonimizzati restano dati personali. Il secondo, di ordine pratico, è l'**onere di gestione** non indifferente che la tecnica comporta: l'attribuzione e la conservazione dei codici, la loro comunicazione ai docenti e il loro aggiornamento a ogni variazione della composizione delle classi, la redazione di documenti che non contengano elementi identificativi, la necessità di ricollegare i documenti agli alunni ogni volta che devono essere trasmessi alle famiglie, agli specialisti o ad altre scuole. Si tratta di un carico organizzativo che molte realtà scolastiche, soprattutto negli istituti di maggiori dimensioni o con segreterie già gravate, non sono in grado di sostenere con la continuità necessaria.

Per queste ragioni riteniamo che la pseudonimizzazione possa essere utilmente adottata dalle scuole che dispongono delle risorse per gestirla, in combinazione con la cifratura, ma che non possa costituire la misura di riferimento. Dedichiamo quindi il resto della nota alla cifratura, che consente di garantire un adeguato livello di protezione con un impegno organizzativo assai più contenuto.

5. La cifratura: di che cosa si tratta

Cifrare un documento significa trasformarne il contenuto, mediante un algoritmo matematico, in una sequenza di dati del tutto incomprensibile, che può essere riportata alla forma originale soltanto da chi dispone della chiave di decifratura. Nelle applicazioni di uso comune la chiave è ricavata da una password scelta dall'utente: chi conosce la password apre il documento e lo legge normalmente; chi non la conosce vede soltanto una richiesta di password e non ha alcun modo di accedere al contenuto.

Un'immagine può aiutare. Un documento conservato in chiaro è come un foglio lasciato su un tavolo: chiunque passi può leggerlo. Un documento cifrato è come lo stesso foglio chiuso in una cassaforte: chi porta via la cassaforte porta via un oggetto, ma non il suo contenuto, finché non ne conosce la combinazione. Gli algoritmi impiegati dai programmi indicati in questa nota, come l'AES a 256 bit, sono gli stessi utilizzati dalle banche e dalle pubbliche amministrazioni e, allo stato delle conoscenze, non possono essere violati con mezzi ragionevoli: la sicurezza del documento dipende quindi soltanto dalla segretezza e dalla robustezza della password.

La cifratura può essere applicata a livelli diversi: al singolo documento, che resta protetto ovunque venga copiato o inviato; a un archivio che raccoglie più documenti; a un intero dispositivo, come una chiavetta USB o il disco di un computer, che diventa illeggibile a chi non conosce la password. Di ciascuno di questi livelli diremo più avanti.

5.1 Che cosa cambia in caso di violazione

Il valore della cifratura emerge proprio nel momento dell'incidente. Se un notebook contenente documenti in chiaro viene rubato, o se un documento in chiaro viene inviato al destinatario sbagliato, i dati sono potenzialmente conoscibili da terzi e la scuola deve, di norma, notificare la violazione al Garante entro 72 ore (art. 33 del GDPR) e, se il rischio per gli interessati è elevato, comunicarla agli interessati stessi (art. 34).

Se invece i documenti sono cifrati secondo lo stato dell'arte e la password non è stata compromessa, i dati restano inaccessibili a chi ne è entrato in possesso. In questo caso l'art. 34, par. 3, lett. a), del GDPR esclude espressamente l'obbligo di comunicazione agli interessati, e le Linee guida 9/2022 del Comitato europeo per la protezione dei dati sulla notifica delle violazioni, così come le Linee guida 01/2021 con i relativi esempi pratici, riconoscono che la perdita o il furto di un dispositivo o di un file cifrato con algoritmi adeguati, la cui chiave non sia stata compromessa, rappresenta il caso tipico in cui è improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone. Ne consegue che **non è dovuta nemmeno la notifica al Garante**, come avverrebbe invece per i file in chiaro.

Le condizioni da verificare. L'esonero dalla notifica non è automatico e presuppone che: (a) la cifratura sia stata applicata con uno degli strumenti e secondo le modalità indicate nelle schede allegate; (b) la password sia robusta, secondo i criteri del [paragrafo 9](#); (c) la password non sia stata compromessa: non si trovasse, ad esempio, nello stesso messaggio del documento, su un foglietto nella custodia del notebook o in un file salvato sul dispositivo sottratto; (d) esista una copia dei documenti, così che la perdita del dispositivo non ne comprometta la disponibilità.

Resta in ogni caso fermo l'obbligo di segnalare l'evento al Dirigente Scolastico e di annotarlo nel **registro delle violazioni** (art. 33, par. 5, del GDPR), indicando le ragioni per le quali si è ritenuto di non procedere alla notifica. È questa documentazione che tutela la scuola in caso di successiva verifica.

6. La gestione della password nei diversi contesti di comunicazione

La cifratura è efficace soltanto se la password è conosciuta da chi deve accedere al documento e da nessun altro. Le modalità di gestione della password variano quindi in funzione dei soggetti coinvolti nella comunicazione.

6.1 Condivisione con i componenti del consiglio di classe

Quando i documenti sono condivisi con l'intero consiglio di classe attraverso il Registro Elettronico o Google Classroom, si utilizza una **password unica del consiglio di classe**. La password è definita all'inizio dell'anno scolastico, di norma nella prima seduta del consiglio, ed è comunicata ai soli componenti in quella sede, a voce, senza essere verbalizzata. Essa **può rimanere invariata per l'intero ciclo di studi della classe**, così da evitare che i documenti degli anni precedenti diventino illeggibili ai docenti che devono consultarli.

I docenti che entrano a far parte del consiglio nel corso del ciclo ricevono la password dal coordinatore di classe, di persona o per telefono. La password deve invece essere sostituita, dandone comunicazione ai componenti con le stesse modalità, qualora vi sia motivo di ritenere che sia stata conosciuta da persone estranee al consiglio. Anche se cifrato, il documento va comunque caricato nell'area riservata ai docenti, verificando ogni volta l'area e i destinatari selezionati.

6.2 Comunicazioni tra docenti

Quando un documento riservato deve essere inviato a uno o più colleghi, ad esempio tramite la posta elettronica istituzionale, e tutti i destinatari sono componenti del medesimo consiglio di classe, **può essere utilizzata la stessa password del consiglio**. In questo caso la password è già nota ai destinatari e non deve essere trasmessa: nel messaggio è sufficiente indicare che il documento è protetto con la password del consiglio, senza riportarla né darne indizi.

Se invece il destinatario non fa parte del consiglio di classe, come può accadere per un docente di un altro ordine di scuola nel passaggio tra gradi o per un referente d'istituto, la password del consiglio non deve essergli comunicata. Il documento va cifrato con una **password diversa**, trasmessa con le modalità indicate al punto successivo.

6.3 Comunicazioni tra docente e genitori

La trasmissione alle famiglie di documenti contenenti dati particolari deve avvenire soltanto quando necessaria e deve riguardare esclusivamente i genitori dell'alunno interessato. Quando possibile, la consegna diretta resta la modalità preferibile. Se si utilizza il Registro Elettronico o la posta elettronica, il documento va indirizzato ai soli genitori dell'alunno, con comunicazione individuale, e cifrato con una **password specifica, diversa da quella del consiglio di classe**, che non deve mai essere comunicata alle famiglie.

La password va trasmessa ai genitori **attraverso un canale separato** rispetto a quello utilizzato per il documento: a voce, per telefono, in occasione di un colloquio o con un messaggio distinto su un diverso mezzo di comunicazione. Non deve mai essere inviata nello stesso messaggio o nella stessa area del Registro in cui si trova il documento, né in un messaggio successivo sullo stesso canale: chi, per errore, avesse accesso al documento avrebbe accesso anche alla password, e la cifratura perderebbe ogni efficacia. È opportuno concordare con la famiglia, al primo invio, il canale da utilizzare per le password.

In sintesi. Consiglio di classe: password unica, definita a inizio anno, valida per l'intero ciclo, mai verbalizzata. Colleghi dello stesso consiglio: stessa password, mai riportata nel messaggio. Genitori e altri destinatari: password specifica, comunicata su un canale separato.

7. Le buone pratiche per ogni condivisione

Alla cifratura vanno affiancate alcune regole di comportamento elementari, che suggeriamo di richiamare nella circolare ai docenti. Dopo aver cifrato un documento occorre sempre **verificare il risultato**, chiudendolo e riaprendolo: la password deve essere richiesta prima che sia visibile qualsiasi parte del contenuto. Se il documento si apre senza password, la cifratura non è stata applicata. Il **nome del file** resta visibile anche quando il contenuto è cifrato, e non deve quindi contenere il nome o il cognome dell'alunno, ma un riferimento neutro. L'**originale non cifrato** va conservato esclusivamente negli spazi indicati dalla scuola, eliminando le copie di lavoro dal computer, dalla cartella dei download e dalle chiavette.

Quanto alla **posta elettronica**, il caso descritto al paragrafo 1 suggerisce una regola precisa: le informazioni riservate non vanno scritte nel corpo del messaggio, che non può essere cifrato con gli strumenti di uso comune, ma in un documento allegato e cifrato, mentre il testo del messaggio deve restare neutro. Prima dell'invio occorre controllare con attenzione i destinatari, senza affidarsi al completamento automatico degli indirizzi. È inoltre opportuno che la scuola assegni alle liste di distribuzione nomi chiaramente distinguibili (ad esempio "docenti-cdc-3B" e "genitori-3B"), valuti se consentire ai docenti l'invio diretto alle liste dei genitori e attivi, ove disponibile, la funzione che consente di annullare l'invio nei secondi successivi.

Vanno infine evitati i **servizi online** che promettono di proteggere o convertire i documenti: per cifrare il file lo si caricherebbe proprio su server di terzi, al di fuori di ogni controllo della scuola. Per l'intero consiglio di classe è opportuno concordare un **unico programma** con cui cifrare i documenti, così che tutti i componenti siano in grado di aprirli: il PDF protetto da password, ottenibile sia con LibreOffice sia con Microsoft Office, ha il vantaggio di poter essere aperto con qualsiasi lettore, anche sullo smartphone.

8. Che cosa fare in caso di errore

Se un documento, anche cifrato, viene caricato nell'area sbagliata, inviato a un destinatario errato o comunque reso accessibile a persone non autorizzate, o se un dispositivo contenente documenti della scuola viene smarrito o sottratto, il docente deve **intervenire immediatamente**, rimuovendo ove possibile il contenuto, e **informare senza ritardo il Dirigente Scolastico**. Nella segnalazione dovrà indicare che cosa è accaduto e quando, quali documenti o dispositivi sono coinvolti, se erano

cifrati e con quale tipo di password (del consiglio di classe o specifica), senza naturalmente riportarla, e se la password possa essere stata conosciuta da altri.

Sarà il Dirigente, con il supporto del DPO, a valutare l'evento e le iniziative da assumere entro le 72 ore previste dall'art. 33 del GDPR. Come si è visto, la cifratura riduce sensibilmente le conseguenze dell'errore e consente di norma di escludere la notifica al Garante, ma **non esonera dalla segnalazione** il dipendente che viene a conoscenza dell'incidente: soltanto una valutazione tempestiva e documentata permette alla scuola di dimostrare di aver agito correttamente.

9. Le caratteristiche di una buona password

Come si è detto, la sicurezza di un documento cifrato dipende quasi interamente dalla qualità della password. Chi entra in possesso di un file o di un dispositivo cifrato può tentare di indovinarne la password senza alcun limite di tentativi, con programmi automatici che provano in sequenza le password più comuni, le parole del vocabolario e le loro combinazioni. Una password breve o prevedibile, come il nome della classe seguito dall'anno, viene individuata in pochi minuti, e la cifratura perde ogni efficacia.

Una buona password deve essere innanzitutto **imprevedibile**, e non contenere quindi il nome della scuola, del plesso, della classe, dell'anno scolastico, di docenti o di alunni, date di nascita o parole ricavabili dal contesto. Deve essere **esclusiva**, e non essere utilizzata anche per altri servizi, come la posta elettronica o i social network. Deve infine essere **facile da ricordare**, perché una password che non si riesce a ricordare finisce inevitabilmente scritta su un foglietto. Sono da evitare, in particolare, le parole comuni completate da numeri o simboli, come «Scuola2026!», che appaiono complesse ma sono fra le prime a essere individuate dai programmi di attacco.

La soluzione che meglio concilia questi requisiti è una password composta da **tre parole scelte a caso e senza legame fra loro, separate da due cifre anch'esse scelte a caso**, ad esempio del tipo tegola7limone3vento (esempio che, essendo pubblicato, non va naturalmente utilizzato). Una password di questo tipo è sufficientemente lunga senza che occorra contarne i caratteri, non compare negli elenchi utilizzati dai programmi di attacco, si ricorda facilmente e si digita senza difficoltà.

Perché la password sia davvero robusta, parole e cifre devono essere **scelte a caso** e non inventate. Chi le sceglie a memoria tende infatti a pescare sempre fra le stesse poche migliaia di parole comuni e a preferire alcune cifre, come l'1, il 2 o il 7, riducendo sensibilmente il numero delle combinazioni da provare. Un metodo semplice consiste nell'aprire un libro a tre pagine diverse e prendere da ciascuna la prima parola che si incontra, scartando articoli, preposizioni e parole collegate alla scuola, e l'ultima cifra del numero di pagina da utilizzare come separatore. La differenza non è trascurabile: tre parole scelte a memoria possono essere individuate in poche ore con un comune computer dotato di una buona scheda grafica; tre parole e due cifre scelte a caso richiedono un tempo che si misura in mesi o in anni.

La regola vale per tutte le password utilizzate per la cifratura: per la **password del consiglio di classe**, che rimane in uso per l'intero ciclo di studi e protegge numerosi documenti, per le **password specifiche** destinate a un singolo invio a una famiglia o a un destinatario esterno al consiglio, e per quelle con cui si cifrano **chiavette, dischi e contenitori**.

In nessun caso la password va scritta nei verbali, nel Registro Elettronico, in Classroom, in file salvati sul computer o in note condivise. Chi ha necessità di annotarla può utilizzare un gestore di password, cioè un programma che conserva le password in forma cifrata, protetto a sua volta da una password robusta.

In sintesi. Tre parole e due cifre scelte a caso, ad esempio da un libro aperto a tre pagine diverse: la prima parola di ogni pagina e l'ultima cifra del numero di pagina come separatore. Mai nomi, classi, anni o parole completate da numeri e simboli. Mai annotata nei verbali o negli spazi condivisi.

10. La cifratura nei diversi contesti

La cifratura trova applicazione in tre contesti diversi, che richiedono strumenti diversi e che descriviamo di seguito. Le procedure operative sono illustrate nelle schede allegate alla presente nota.

10.1 La cifratura dei dispositivi di memorizzazione

Le chiavette USB e i dischi esterni sono i dispositivi più esposti al rischio di smarrimento. Il nostro consiglio è di limitarne l'uso per i documenti riservati, preferendo le piattaforme della scuola; ove il loro impiego sia necessario, occorre utilizzare esclusivamente dispositivi **cifrati per intero**, così che qualsiasi file vi venga copiato risulti automaticamente protetto.

Sui computer con Windows nelle edizioni Pro ed Education, normalmente in uso nelle scuole, la soluzione più semplice è **BitLocker To Go**, funzione integrata nel sistema operativo che cifra l'intera chiavetta con una password ([scheda D](#)). La chiavetta così protetta può essere aperta su qualsiasi computer Windows, anche nell'edizione Home, inserendo la password. Chi utilizza un Mac può cifrare la chiavetta direttamente dal Finder, ma il dispositivo sarà leggibile soltanto sui Mac ([scheda F](#)). Quando la chiavetta deve essere utilizzata su sistemi diversi, o su computer Windows Home che non consentono di attivare BitLocker, si può ricorrere al programma gratuito **VeraCrypt** ([scheda G](#)). Esistono infine in commercio chiavette dotate di cifratura hardware e tastierino per l'inserimento del codice, che non richiedono alcun programma e rappresentano una soluzione valida per il personale che deve trasportare con frequenza documenti riservati.

10.2 La cifratura del disco dei computer e dei notebook

La cifratura del disco protegge tutti i dati presenti sul computer in caso di furto o smarrimento: chi sottrae il dispositivo, anche smontandone il disco, non può leggerne il contenuto. È una misura particolarmente importante per i notebook, per loro natura trasportabili, ma che suggeriamo di adottare per tutti i computer della scuola sui quali siano presenti dati personali, a partire da quelli delle segreterie.

Per i **computer della scuola** la cifratura va attivata a cura dell'amministratore di sistema, che ne custodisce le chiavi di ripristino secondo procedure documentate: su Windows mediante **BitLocker** ([scheda E](#)), su Mac mediante **FileVault** ([scheda F](#)). Si tratta di funzioni integrate nel sistema operativo, che una volta attivate non richiedono alcun intervento da parte dell'utente e non rallentano apprezzabilmente il funzionamento del computer. Sui computer più recenti con Windows 11 la cifratura potrebbe essere già attiva: la [scheda E](#) indica come verificarlo. Perché la protezione sia effettiva, l'accesso al computer deve essere a sua volta protetto da una password robusta e il blocco automatico dello schermo deve essere attivo.

La cifratura dei computer della scuola, e in particolare di quelli della segreteria, che conservano la maggior parte dei dati dell'istituto, richiede tuttavia alcune cautele organizzative, che è bene il Dirigente Scolastico concordi con l'amministratore di sistema. Il rischio principale è la **perdita della chiave di ripristino**: BitLocker la richiede non soltanto in caso di password dimenticata, ma anche in occasione di aggiornamenti del firmware, di modifiche alla configurazione o di sostituzione di componenti, e senza di essa i dati non sono più recuperabili. Le chiavi devono quindi essere raccolte e custodite in modo centralizzato e documentato, con una copia accessibile al Dirigente, e occorre verificare dove si trovino quelle dei computer sui quali la cifratura è stata attivata automaticamente dal sistema operativo, che potrebbero essere state salvate nell'account personale di chi ha configurato il computer. È inoltre opportuno procedere dopo un censimento dei dispositivi, verificando l'esistenza di copie di sicurezza funzionanti, sperimentando la procedura su un singolo computer ed evitando i periodi di maggiore attività degli uffici; sui computer più datati la cifratura iniziale può richiedere alcune ore. Occorre infine ricordare che la cifratura del disco protegge i dati quando il computer è spento, ma non quando è acceso e in uso, né protegge da virus e attacchi informatici, e

che non si estende ai documenti conservati su server o dischi di rete, i quali richiedono misure proprie. Un vantaggio spesso trascurato riguarda la dismissione dei computer: la cancellazione della chiave rende i dati di un disco cifrato definitivamente illeggibili, semplificando le procedure di cancellazione sicura.

I docenti che utilizzano un computer personale per lavorare con documenti della scuola possono proteggerne il disco con gli stessi strumenti, seguendo le schede [E](#) ed [F](#) e custodendo con cura la chiave di ripristino, senza la quale, in caso di guasto o di smarrimento della password, i dati andrebbero perduti. Il docente che non intenda cifrare il disco del proprio computer dovrà comunque **cifrare i documenti contenenti dati riconducibili alla scuola** che vi conserva, singolarmente con le funzioni dei programmi di videoscrittura (schede [A](#) e [B](#)) o raccogliendoli in un archivio o in un contenitore cifrato (schede [C](#) e [G](#)). Resta preferibile, in ogni caso, che i documenti riservati siano conservati negli spazi istituzionali messi a disposizione dalla scuola, e non sui dispositivi personali.

10.3 La cifratura dei file da inviare o condividere

I documenti da inviare per posta elettronica o da condividere sul Registro Elettronico, su Classroom o negli spazi condivisi vanno cifrati singolarmente prima dell'invio o del caricamento, con la password definita secondo le indicazioni dei paragrafi 6 e 9. È questo il livello di cifratura più importante, perché il documento resta protetto ovunque venga copiato o inoltrato, e anche nelle mani di un destinatario errato.

Per i documenti di testo e i fogli di calcolo si utilizzano le funzioni integrate nei programmi di uso comune: **LibreOffice** ([scheda A](#)), suite gratuita che consente di esportare PDF protetti con cifratura AES-256 e di salvare documenti con password, e **Microsoft Office** ([scheda B](#)), disponibile in molte scuole attraverso le licenze Microsoft 365 per l'istruzione. Per i file di altro formato, come le scansioni e le immagini, o per inviare più documenti insieme, si utilizza il programma gratuito **7-Zip** ([scheda C](#)), che raccoglie i file in un archivio cifrato, nascondendone anche i nomi.

11. La regolamentazione della materia nella scuola

Le indicazioni contenute nella presente nota producono effetti concreti soltanto se diventano regole conosciute e vincolanti per tutto il personale. La cifratura dei documenti, la gestione delle password nei consigli di classe, il divieto di utilizzare canali non istituzionali e l'obbligo di segnalare tempestivamente ogni errore sono comportamenti che il Dirigente Scolastico, in qualità di rappresentante del titolare del trattamento, deve richiedere formalmente. È inoltre la loro formalizzazione a consentire alla scuola di dimostrare, in caso di verifica, di aver adottato misure tecniche e organizzative adeguate, come richiesto dagli artt. 5, par. 2, e 32 del GDPR, e di aver impartito al personale autorizzato istruzioni specifiche, ai sensi dell'art. 29 del GDPR e dell'art. 2-quaterdecies del Codice.

Non riteniamo tuttavia opportuno appesantire il corpo documentale della scuola con un regolamento specifico. Le scuole dispongono già di numerosi regolamenti, disciplinari e procedure, e un ulteriore atto di questo tipo, con le relative procedure di adozione, rischierebbe di restare poco conosciuto e poco applicato. È sufficiente, a nostro avviso, un **unico atto del Dirigente Scolastico che detti al personale disposizioni puntuali e operative**, emesso nella forma consueta della circolare. Così le regole raggiungono direttamente docenti e personale ATA, possono essere aggiornate con facilità e valgono come integrazione delle istruzioni già impartite agli autorizzati al trattamento, senza la necessità di ulteriori atti.

A questo scopo mettiamo a disposizione delle scuole un [modello di disposizione del Dirigente Scolastico al personale](#) sulla riservatezza dei documenti e delle comunicazioni. Si tratta, appunto, di un **modello**, che ciascuna scuola dovrà personalizzare in funzione delle regole che intende introdurre, dell'organizzazione dei propri uffici e dei consigli di classe e degli strumenti informatici di cui dispone. Nella versione proposta il modello definisce gli strumenti di condivisione consentiti, l'obbligo di cifratura, le caratteristiche e la gestione delle password, i compiti dei coordinatori di classe e del personale di segreteria e le modalità di segnalazione degli incidenti. Alla disposizione

vanno allegate le [schede operative A–G](#), che descrivono passo per passo le procedure di cifratura dei documenti e dei dispositivi e che il personale potrà consultare al momento del bisogno.

L'adozione della disposizione è necessaria soprattutto nelle scuole in cui oggi i documenti contenenti dati particolari circolano senza regole definite, attraverso la posta elettronica, le chiavette o le piattaforme, affidati alle abitudini dei singoli docenti. Le indicazioni della presente nota non riguardano invece le scuole che abbiano già adottato misure più rigorose, ad esempio consentendo l'accesso a tali documenti soltanto mediante presa visione delle copie cartacee custodite a scuola e vietandone la condivisione su piattaforme telematiche. In questi casi la disposizione proposta non è necessaria, perché la riservatezza è già garantita dalla scelta di non far circolare i documenti in formato digitale. Restano tuttavia valide, anche per queste scuole, le indicazioni del § 10.2 sulla cifratura dei computer: i documenti che non circolano fra i docenti vengono comunque redatti, protocollati e conservati in formato digitale sui computer della segreteria, che sono esposti al rischio di furto al pari di qualsiasi altro dispositivo. Per le altre scuole suggeriamo di emanare la disposizione in tempo utile per le prime sedute dei consigli di classe, nelle quali dovrà essere definita la password di cifratura di ciascun consiglio.

12. Note collegate e riferimenti

[DPO 104/2026](#) – Registro Elettronico all'avvio dell'anno scolastico 2026/27: accessi, aree riservate e dati particolari degli alunni;

[DPO 98/2025](#) – Condivisione di dati e documenti nel consiglio di classe;

[DPO 36/2025](#) – Indicazioni operative per l'uso del registro elettronico.

Normativa e linee guida:

Regolamento (UE) 2016/679, artt. 4, n. 5 e n. 12, 32, 33 e 34;

Comitato europeo per la protezione dei dati (EDPB), Linee guida 9/2022 sulla notifica delle violazioni dei dati personali ai sensi del GDPR (versione 2.0 del 28 marzo 2023);

Comitato europeo per la protezione dei dati (EDPB), Linee guida 01/2021 su esempi riguardanti la notifica di una violazione dei dati personali;

Garante per la protezione dei dati personali, Provvedimento del 27 febbraio 2025 [doc. web n. 10126123] – pubblicazione del PEI sul registro elettronico.

Allegati – Schede operative:

- [Scheda A – Cifrare i documenti con LibreOffice](#)
- [Scheda B – Cifrare i documenti con Microsoft Office](#)
- [Scheda C – Cifrare file e cartelle con 7-Zip](#)
- [Scheda D – Cifrare una chiavetta USB con BitLocker To Go \(Windows\)](#)
- [Scheda E – Cifrare il disco del computer con BitLocker \(Windows\)](#)
- [Scheda F – Cifrare il disco e le chiavette USB su Mac \(FileVault e Finder\)](#)
- [Scheda G – Creare un contenitore cifrato con VeraCrypt \(Windows, Mac, Linux\)](#)

Cifrare i documenti con LibreOffice

Documenti di testo e PDF – Windows, macOS, Linux – gratuito

Prima di iniziare

LibreOffice va scaricato esclusivamente dal sito ufficiale it.libreoffice.org e mantenuto aggiornato. Per la cifratura dei PDF è necessaria la **versione 25.8 o successiva**, che consente di esportare in formato PDF 2.0 con cifratura AES-256. La versione installata si verifica dal menu **Aiuto** → **Informazioni su LibreOffice** (su Mac: **LibreOffice** → **Informazioni su LibreOffice**).

La procedura A1 produce un PDF protetto, apribile con qualsiasi lettore di PDF: è la soluzione consigliata per i documenti da consultare. La procedura A2 protegge il documento di testo modificabile, utile quando più colleghi devono lavorare sullo stesso file.

Procedura A1 – Esportare un PDF protetto da password (consigliata)

1. Aprire il documento in LibreOffice Writer.
2. Dal menu scegliere **File** → **Esporta come** → **Esporta come PDF...**
3. Nella scheda **Generale**, nel menu a tendina della versione, selezionare **PDF 2.0**, che garantisce la cifratura AES-256. Non selezionare le versioni PDF/A, che non ammettono la protezione con password.
4. Aprire la scheda **Sicurezza** e premere il pulsante **Imposta password...**
5. Nella sezione relativa alla **password di apertura** inserire la password e ripeterla nel campo di conferma. La sezione relativa alla password dei permessi può essere lasciata vuota: da sola non protegge il contenuto.
6. Premere **OK**, poi **Esporta**, scegliere la cartella e il nome del file e premere **Salva**.

Procedura A2 – Salvare il documento di testo con password

1. Dal menu scegliere **File** → **Salva con nome...** e mantenere il formato **Documento di testo ODF (.odt)**.
2. Nella parte inferiore della finestra spuntare la casella **Salva con password** e premere **Salva**.
3. Inserire la password nel campo relativo alla **password di apertura del file** e ripeterla per conferma. Non è necessario impostare la password di modifica, che da sola non protegge il contenuto.
4. Premere **OK**. Il documento potrà essere aperto solo inserendo la password; la protezione resta attiva a ogni salvataggio successivo.

Da ricordare. PDF 2.0 con password di apertura, oppure “Salva con password”. Non utilizzare la sola password dei permessi o di modifica. Verificare sempre, riaprendo il file, che la password venga richiesta.

Cifrare i documenti con Microsoft Office

Documenti Word, fogli Excel e PDF – Windows e Mac

Prima di iniziare

La cifratura richiede l'applicazione **Word installata sul computer** (Microsoft 365 o Office 2016 e versioni successive). Word per il web, cioè la versione che si usa nel browser, non consente di impostare la password di apertura, mentre permette di aprire i documenti già protetti. Il documento va salvato nel formato **.docx**: il vecchio formato .doc utilizza una protezione non più adeguata.

Procedura B1 – Proteggere il documento Word con password (consigliata)

1. Aprire il documento in Word.
2. Dal menu scegliere **File** → **Informazioni** → **Proteggi documento** → **Crittografia con password**.
3. Inserire la password e premere **OK**; ripeterla nella finestra successiva e premere di nuovo **OK**.
4. Salvare il documento (**File** → **Salva** oppure Ctrl+S): la protezione diventa effettiva con il salvataggio.

Su Mac la stessa funzione si trova nella scheda **Revisione** → **Proteggi documento**, impostando la password nel campo relativo all'apertura del documento. Per i fogli Excel il percorso è analogo: **File** → **Informazioni** → **Proteggi cartella di lavoro** → **Crittografia con password**.

Procedura B2 – Salvare un PDF protetto da password

1. Dal menu scegliere **File** → **Salva con nome** e, come tipo di file, selezionare **PDF**.
2. Premere il pulsante **Opzioni...**, spuntare la casella **Crittografia il documento con una password** e premere **OK**.
3. Premere **Salva**: Word chiederà di inserire la password e di ripeterla. Per i PDF Word ammette password di non più di 32 caratteri, limite sufficiente per una password composta secondo i criteri del § 9; se la password scelta lo supera, occorre utilizzare la procedura B1.

Funzioni da non utilizzare

Non cifrano il documento, che resta leggibile a chiunque lo apra: **Limita modifica** e **Segna come finale** (scheda Revisione); la sola **password di modifica** impostabile da Salva con nome → Strumenti → Opzioni generali; la **protezione del foglio** di Excel. Se il documento si trova in una cartella sincronizzata con **OneDrive**, occorre verificare che la versione non cifrata non resti disponibile nella cronologia delle versioni.

Da ricordare. File → Informazioni → Proteggi documento → Crittografia con password, oppure PDF con l'opzione "Crittografia il documento con una password". Verificare sempre, riaprendo il file, che la password venga richiesta.

Cifrare file e cartelle con 7-Zip

Archivi cifrati di file di qualsiasi formato – Windows – gratuito

Quando utilizzarlo

7-Zip è utile per proteggere **file di qualsiasi formato** (scansioni, immagini, fogli di calcolo) o **più file insieme**, raccolti in un unico archivio cifrato da inviare per posta elettronica o da condividere, e per proteggere i documenti della scuola conservati su un computer personale il cui disco non sia cifrato. Il programma va scaricato **esclusivamente dal sito ufficiale 7-zip.org**, diffidando dei siti con nomi simili.

Chi riceve l'archivio deve avere 7-Zip installato: Esplora file di Windows non è in grado di aprire gli archivi cifrati. I colleghi che utilizzano un Mac possono aprirli con il programma gratuito Keka.

Procedura – Creare un archivio cifrato

1. Selezionare il file, i file o la cartella da proteggere, fare clic con il tasto destro e scegliere **7-Zip** → **Aggiungi all'archivio...** In Windows 11 la voce compare dopo aver scelto **Mostra altre opzioni**.
2. Nel campo **Archivio** indicare un nome neutro, che non contenga il nome dell'alunno.
3. Come **formato dell'archivio** selezionare **7z**.
4. Nella sezione **Crittografia** inserire la password, ripeterla e verificare che il **metodo di crittografia** sia **AES-256**.
5. Spuntare la casella **Crittografa i nomi dei file**, così che senza password non sia visibile nemmeno l'elenco dei documenti contenuti.
6. Premere **OK**: nella stessa cartella verrà creato il file con estensione .7z. Eliminare quindi gli originali non cifrati, se non devono essere conservati sul dispositivo.

Aprire un archivio cifrato

Fare clic con il tasto destro sull'archivio, scegliere **7-Zip** → **Estrai file...** e inserire la password. Terminata la consultazione, **eliminare i file estratti**, in particolare sui computer condivisi.

Da evitare

Il formato **zip** con metodo **ZipCrypto**, che offre una protezione debole; la funzione di Windows **Invia a** → **Cartella compressa**, che non consente di impostare alcuna password; gli archivi creati senza spuntare **Crittografa i nomi dei file**.

Da ricordare. Formato 7z, metodo AES-256, casella "Crittografa i nomi dei file" spuntata. Verificare che la password venga richiesta già per visualizzare il contenuto dell'archivio.

Cifrare una chiavetta USB con BitLocker To Go

Chiavette USB e dischi esterni – Windows 10 e 11 Pro, Education, Enterprise

Prima di iniziare

BitLocker To Go è una funzione integrata in Windows che cifra per intero una chiavetta USB o un disco esterno: da quel momento ogni file copiato sulla chiavetta è automaticamente protetto. La cifratura può essere **attivata** soltanto sulle edizioni Pro, Education ed Enterprise di Windows, normalmente in uso sui computer della scuola; la chiavetta cifrata può invece essere **aperta e utilizzata** su qualsiasi computer Windows, anche nell'edizione Home, inserendo la password. I Mac non sono in grado di leggerla senza programmi aggiuntivi: in questo caso si veda la [scheda G](#).

Prima di procedere è opportuno salvare altrove una copia dei file già presenti sulla chiavetta. La procedura può richiedere da pochi minuti a oltre un'ora, a seconda della capacità del dispositivo, e durante l'operazione la chiavetta **non deve essere rimossa**.

Procedura – Attivare BitLocker sulla chiavetta

1. Inserire la chiavetta, aprire **Esplora file** e selezionare **Questo PC**.
2. Fare clic con il tasto destro sulla chiavetta e scegliere **Attiva BitLocker** (in Windows 11, dopo aver scelto **Mostra altre opzioni**). In alternativa: **Pannello di controllo** → **Sistema e sicurezza** → **Crittografia unità BitLocker**, sezione **Unità dati rimovibili – BitLocker To Go**.
3. Spuntare **Usa una password per sbloccare l'unità**, inserire la password e ripeterla; premere **Avanti**.
4. Scegliere come salvare la **chiave di ripristino**, un codice di 48 cifre che consente di aprire la chiavetta se la password viene dimenticata: **Salva in un file** (da conservare in un luogo sicuro, mai sulla chiavetta stessa) oppure **Stampa la chiave di ripristino**. Sui dispositivi della scuola, seguire le indicazioni dell'amministratore di sistema.
5. Alla domanda sulla porzione da crittografare scegliere **Crittografa l'intera unità** se la chiavetta è già stata utilizzata (i file cancellati potrebbero altrimenti restare leggibili), oppure **Crittografa solo lo spazio utilizzato** se è nuova.
6. Scegliere la **Modalità compatibile**, adatta alle unità da utilizzare su computer diversi, e premere **Avvia crittografia**. Attendere il messaggio di completamento.

Utilizzare la chiavetta cifrata

Inserendo la chiavetta in un computer Windows compare la richiesta di password: dopo averla inserita, la chiavetta si utilizza normalmente. Non spuntare l'opzione di sblocco automatico sui computer condivisi. Al termine, rimuovere la chiavetta con la funzione **Rimozione sicura dell'hardware**: una volta estratta, torna a essere protetta.

Da ricordare. Password di tre parole e due cifre scelte a caso ([§ 9 della nota](#)), diversa da quella del consiglio di classe; chiave di ripristino conservata separatamente dalla chiavetta; "Crittografa l'intera unità" per le chiavette già utilizzate.

Cifrare il disco del computer con BitLocker

Computer e notebook con Windows 10 e 11

Prima di iniziare

La cifratura del disco protegge tutti i dati del computer in caso di furto o smarrimento. Sui **computer della scuola** l'attivazione e la custodia delle chiavi di ripristino competono all'**amministratore di sistema**: questa scheda è rivolta principalmente ai docenti che intendano proteggere il proprio computer personale. Prima di procedere è opportuno eseguire una copia di sicurezza dei dati e collegare il notebook all'alimentazione.

Windows offre due funzioni, a seconda dell'edizione: **BitLocker**, nelle edizioni Pro ed Education, e **Crittografia dispositivo**, disponibile anche nell'edizione Home sui computer che soddisfano i requisiti hardware. L'edizione installata si verifica in **Impostazioni** → **Sistema** → **Informazioni su**, alla voce **Edizione**.

Verificare se la cifratura è già attiva

Sui computer più recenti, installati o ripristinati con Windows 11 versione 24H2 o successiva, la cifratura può essere già attiva. Aprire **Impostazioni** → **Privacy e sicurezza** → **Crittografia dispositivo**: se l'interruttore è attivo, il disco è già cifrato. In questo caso occorre soltanto assicurarsi di disporre della chiave di ripristino, che nei computer personali è di norma salvata nell'account Microsoft (consultabile all'indirizzo account.microsoft.com/devices/recoverykey). Se la voce Crittografia dispositivo non compare, il computer non supporta questa funzione e occorre utilizzare BitLocker, se disponibile, o cifrare i singoli documenti (schede [A](#), [B](#), [C](#) e [G](#)).

Procedura E1 – Windows Home: Crittografia dispositivo

1. Accedere a Windows con un **account Microsoft**, necessario per il salvataggio automatico della chiave di ripristino.
2. Aprire **Impostazioni** → **Privacy e sicurezza** → **Crittografia dispositivo** e attivare l'interruttore.
3. Verificare, all'indirizzo indicato sopra, che la chiave di ripristino sia stata salvata, annotandone eventualmente una copia da conservare in luogo sicuro, separato dal computer.

Procedura E2 – Windows Pro ed Education: BitLocker

1. Aprire **Pannello di controllo** → **Sistema e sicurezza** → **Crittografia unità BitLocker** (oppure cercare "Gestisci BitLocker" dal menu Start).
2. In corrispondenza dell'unità del sistema operativo (di norma C:) scegliere **Attiva BitLocker**.
3. Scegliere come salvare la **chiave di ripristino**: nell'account Microsoft, in un file su un'unità esterna o stampata. Non salvarla sul disco che si sta cifrando.
4. Scegliere **Crittografia l'intera unità** per un computer già in uso e la **Nuova modalità di crittografia**, adatta ai dischi interni.
5. Lasciare spuntata l'opzione **Esegui controllo di sistema BitLocker**, premere **Continua** e riavviare il computer quando richiesto. La cifratura prosegue in background: il computer può essere utilizzato normalmente.

Da ricordare. La cifratura del disco protegge i dati quando il computer è spento o bloccato: l'accesso a Windows deve essere protetto da una password robusta, diversa da quelle utilizzate per altri servizi, e il blocco automatico dello schermo deve essere attivo. Senza la chiave di ripristino, in caso di guasto, i dati non sono recuperabili.

Cifrare il disco e le chiavette USB su Mac

FileVault e cifratura dal Finder – macOS

Procedura F1 – Cifrare il disco con FileVault

FileVault è la funzione di macOS che cifra l'intero disco del Mac. Sui computer della scuola va attivata a cura dell'amministratore di sistema; sui Mac personali può essere attivata dal docente. È opportuno eseguire prima una copia di sicurezza con Time Machine.

1. Aprire il menu **Apple** → **Impostazioni di Sistema** → **Privacy e sicurezza**.
2. Scorrere fino alla sezione **FileVault** e premere **Attiva...**; inserire la password dell'utente quando richiesta.
3. Scegliere come consentire lo sblocco del disco in caso di password dimenticata: tramite l'**account iCloud** oppure mediante una **chiave di recupero**. In quest'ultimo caso, trascrivere la chiave e conservarla in un luogo sicuro, separato dal computer.
4. Premere **Continua**. La cifratura procede in background mentre il Mac viene utilizzato normalmente; lo stato di avanzamento è visibile nella stessa sezione.

Procedura F2 – Cifrare una chiavetta USB dal Finder

Una chiavetta cifrata con questa procedura è leggibile **soltanto sui Mac**. Per le chiavette da utilizzare anche su Windows si veda la [scheda G](#).

1. Inserire la chiavetta e individuarla nella barra laterale del **Finder**.
2. Fare clic con il tasto destro (o Ctrl+clic) sulla chiavetta e scegliere **Codifica "nome della chiavetta"...**
3. Inserire la password, ripeterla e aggiungere un suggerimento che non la renda intuibile; premere **Codifica disco**.
4. Se la voce Codifica non compare, la chiavetta ha un formato non compatibile: occorre inizializzarla con **Utility Disco**, scegliendo il formato **APFS (codificato)**, dopo aver salvato altrove i file che contiene, che verranno cancellati.

Da ricordare. FileVault protegge i dati quando il Mac è spento o bloccato: l'account utente deve essere protetto da una password robusta, diversa da quelle utilizzate per altri servizi, e il blocco dello schermo deve essere attivo. Conservare la chiave di recupero separatamente dal computer.

Creare un contenitore cifrato con VeraCrypt

Chiavette USB e computer personali – Windows, macOS, Linux – gratuito e open source

Quando utilizzarlo

VeraCrypt è un programma gratuito e open source che crea un **contenitore cifrato**: un file che, una volta aperto con la password, si comporta come un'unità disco aggiuntiva nella quale copiare e modificare i documenti, che vengono cifrati e decifrati automaticamente. È utile per le chiavette USB da utilizzare su sistemi diversi (Windows e Mac) e per i docenti che non possono o non vogliono cifrare il disco del proprio computer personale ma devono conservarvi documenti della scuola.

Il programma va scaricato **esclusivamente dal sito ufficiale veracrypt.io**. L'installazione richiede i diritti di amministratore, e VeraCrypt deve essere installato su ogni computer sul quale si intende aprire il contenitore; su Mac richiede anche il componente gratuito macFUSE. Per queste ragioni è indicato soprattutto per i dispositivi personali.

Procedura G1 – Creare il contenitore

1. Avviare VeraCrypt e premere **Crea un volume**.
2. Scegliere **Crea un file contenitore cifrato** e poi **Volume VeraCrypt standard**; premere **Avanti**.
3. Premere **Seleziona file...**, scegliere la posizione (ad esempio la chiavetta USB o la cartella Documenti) e indicare un nome neutro per il contenitore; premere **Salva** e poi **Avanti**.
4. Lasciare le impostazioni predefinite di cifratura (**AES**, hash **SHA-512**) e premere **Avanti**.
5. Indicare la **dimensione** del contenitore, adeguata ai documenti da conservare (ad esempio 2 GB), e premere **Avanti**.
6. Inserire la **password**, scelta secondo i criteri del [§ 9 della nota](#) (tre parole e due cifre scelte a caso), e ripeterla; premere **Avanti**.
7. Come file system scegliere **exFAT**, se il contenitore deve essere aperto anche su Mac, oppure **NTFS** per l'uso sul solo Windows. Muovere il mouse in modo casuale all'interno della finestra finché la barra non è completa, quindi premere **Formatta** e, al termine, **Esci**.

Procedura G2 – Aprire e chiudere il contenitore

1. Avviare VeraCrypt, selezionare una lettera di unità libera nell'elenco e premere **Seleziona file...** per scegliere il contenitore.
2. Premere **Monta** e inserire la password: il contenitore compare in Esplora file (o nel Finder) come una normale unità disco, nella quale copiare, aprire e modificare i documenti.
3. Al termine del lavoro tornare in VeraCrypt, selezionare l'unità e premere **Smonta**: i documenti tornano a essere inaccessibili senza password.

Da ricordare. VeraCrypt non consente il recupero di una password dimenticata: senza di essa i documenti sono perduti. Conservare una copia di sicurezza dei documenti negli spazi istituzionali e smontare sempre il contenitore al termine del lavoro.