



ISTITUTO STATALE di ISTRUZIONE SUPERIORE DELLA BASSA FRIULANA

Via mons. A. Ramazzotti, 41 – 33052 Cervignano del Friuli tel. 0431.31261 C.F.90011220309
<http://www.isisbassafriulana.edu.it/> e mail udis01300a@istruzione.it – pec udis01300a@pec.istruzione.it



Visto il Regolamento Europeo 2016/679 in relazione al trattamento dei dati;
Visto il Decreto Legislativo 7 marzo 2005, n. 82 Codice dell'amministrazione digitale sulla dematerializzazione di documenti amministrativi;
Tenuto conto dell'esigenza, accelerata dall'epidemia, di effettuare riunioni on line e di condividere anche documenti riservati;
Allo scopo di sfruttare gli strumenti tecnologici per una efficace collaborazione fra i docenti chiamati ad elaborare collegialmente documenti riservati;
Considerata l'esigenza di consultare on line documenti riservati;
Considerata l'esigenza di redigere in modo condiviso e sottoporre ai genitori e all'equipe multi-specialistica documenti quali PDP e PEI;
Preso atto del parere favorevole del Collegio dei Docenti espresso nella seduta del 26/02/2021.

IL CONSIGLIO D'ISTITUTO DELL'ISIS DELLA BASSA FRIULANA Nella seduta dell'8 marzo 2021 adotta il seguente **REGOLAMENTO PER LA CONDIVISIONE ON LINE DI DOCUMENTI RISERVATI**

Art. 1 Protezione dei documenti digitali mediante crittografia

Documenti riservati contenenti informazione sulla salute degli studenti e altri documenti elaborati dal Consiglio di Classe o da singoli docenti che fanno riferimento a situazioni specifiche di studenti possono essere detenuti anche in forma digitale, a patto che:

- I file siano crittografati o protetti da password personale
OPPURE
- I file siano memorizzati su supporti crittografati o protetti da password personale

Al termine dell'utilizzo i file devono essere cancellati come previsto dall'Art. 4.

Art 2 Trasmissione di documenti riservati

I documenti riservati possono essere trasmessi solo tramite posta elettronica istituzionale, devono essere crittografati come previsto all'Art. 1, la password per la decodifica del documento protetto deve essere trasmessa con modalità diversa da quella usata per la trasmissione del documento (esempio, documento trasmesso via email, password trasmessa via cellulare).

Art. 3 Elaborazione condivisa di documenti riservati

Per l'elaborazione condivisa dei documenti riservati si deve utilizzare esclusivamente la piattaforma Microsoft Office 365 (ad esempio utilizzando Teams, SharePoint e OneDrive) adottata ufficialmente dall'istituto, utilizzando le proprie credenziali istituzionali per l'autenticazione.

I permessi di accesso andranno limitati al solo Team del Consiglio di Classe coinvolto, in modo che possano accedere i soli docenti della classe.

Art 4 Conservazione dei documenti riservati

I documenti riservati definitivi dovranno essere conservati dall'Assistente Amministrativa incaricata del trattamento di tali dati.

I file utilizzati dai docenti per l'elaborazione dovranno essere eliminati subito dopo la trasmissione della documentazione all'assistente amministrativa di cui al comma precedente. I file memorizzati nella piattaforma rimarranno a disposizione del CdC per tutto l'A.S. e a fine anno scolastico, sarà tutto archiviato automaticamente, seguendo le policy di data retention impostate sulla piattaforma stessa.

Allegati:

Descrizione per proteggere un file con crittografia

GUIDA ALLA CRITTOGRAFIA DI FILE

IN OFFICE 365

v.1 – 06/03/21

INDICE

1.	Necessità della crittografia dei file.....	1
2.	Installare Microsoft Office 365	2
3.	Crittografare un file in Office 365.....	2
4.	Togliere la crittografia a un file in Office 365.....	3
5.	Crittografare un file su Windows 10	4

1. Necessità della crittografia dei file

L'ISIS della Bassa Friulana stabilisce un regolamento per la gestione dei documenti digitali che contengono informazioni riservate sugli studenti.

Crittografare un file significa codificarlo in modo che sia possibile accedervi e visionarlo solo inserendo una password¹.

L'obiettivo della crittografia è mantenere al sicuro i documenti riservati per tutto il tempo in cui è opportuno conservarli sui propri dispositivi e quando si rende necessario inviarli o condividerli con altre persone.

Si precisa pertanto che:

- **se un file viene caricato su Microsoft Teams** all'interno di un team in cui tutti i membri hanno diritto ad accedere al documento, il file è al sicuro in quanto vi si può accedere solo tramite un account istituzionale con password personale;
- **se un file viene salvato su un dispositivo personale**, soprattutto se di tipo portatile (pc portatile, tablet, smartphone), è opportuno crittografare il file, o meglio ancora crittografare l'intero dispositivo;

¹ Come stabilito dal regolamento, la password deve essere comunicata ai destinatari con un mezzo diverso da quello con cui si invia loro il file crittografato.

- **in caso di furto/smarrimento di un dispositivo portatile**, è fatto obbligo di informare l'Animatore Digitale o il Responsabile Tecnico dell'Istituto, che provvederanno a terminare tutte le sessioni attive sul dispositivo (in altre parole, chiudere l'accesso a Teams, alla mail scolastica e a tutti i servizi Microsoft per quello specifico dispositivo);
- **per inviare un documento riservato** è fatto obbligo di utilizzare esclusivamente gli indirizzi e-mail istituzionali, sia per il mittente che per i destinatari;
- **nel caso un documento riservato venga inviato all'esterno dell'organizzazione scolastica** o comunque si renda disponibile a persone che non hanno diritto ad accedervi, il responsabile è passibile di provvedimenti disciplinari.

2. Installare Microsoft Office 365

Questa guida fa riferimento alle versioni aggiornate dei programmi di Office 365.

Si ricorda che l'Istituto fornisce a tutti i docenti una licenza per i prodotti Microsoft che permette di scaricare sui propri dispositivi l'intero pacchetto Office 365 (Word, Excel, Powerpoint, ecc.).

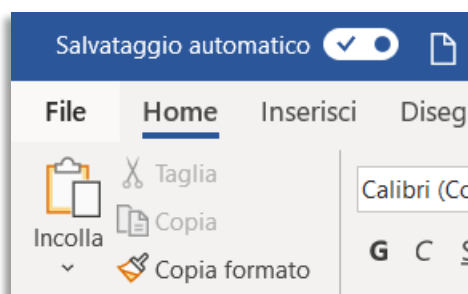
Per installare Office 365 seguire la seguente procedura:

- aprire il sito www.office.com;
- cliccare su "Accedi" in alto a destra e inserire le credenziali scolastiche (mail d'istituto e password scelta dall'utente per accedere a Teams, Outlook e tutti i servizi Office 365);
- cliccare in alto a destra su "Installa Office" e poi su "App di Office 365", come nella figura a fianco.

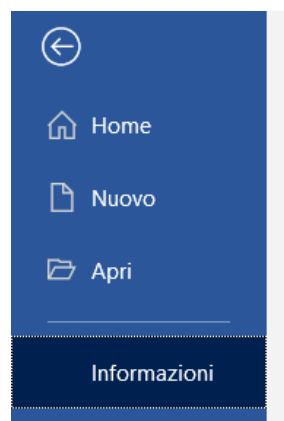


3. Crittografare un file in Office 365

Per crittografare un file in Office 365 seguire la seguente procedura, qui mostrata per Word e analoga per Excel, PowerPoint, ecc.

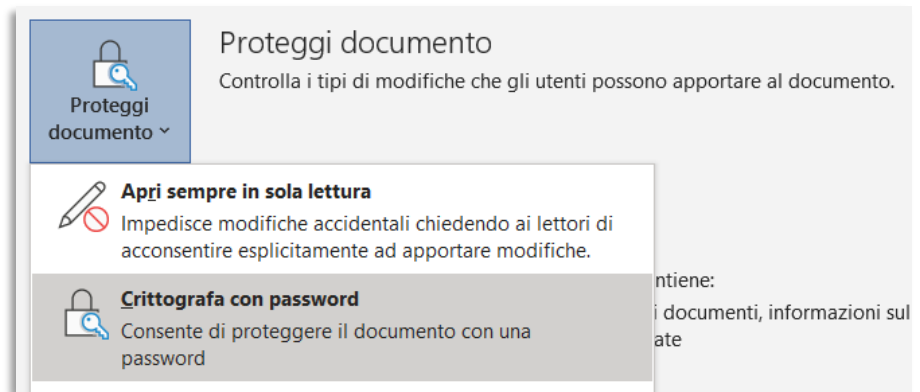


Aprire il menu File in alto a sinistra



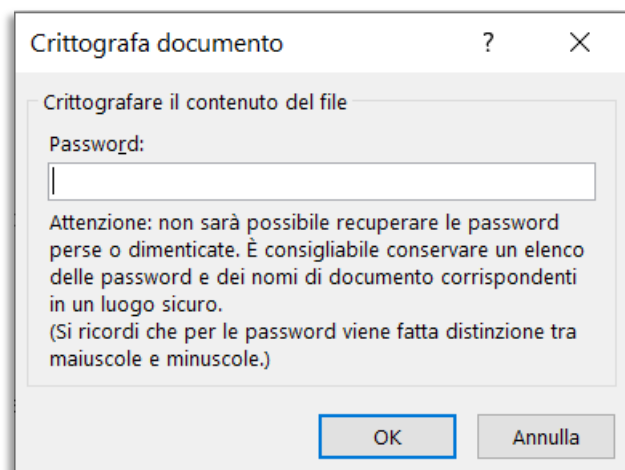
Cliccare su Informazioni

Cliccare sul pulsante “Proteggi documento” e poi su “Crittografia con password”.

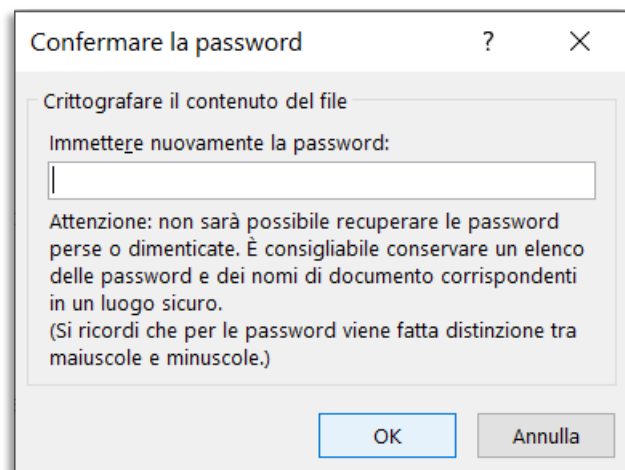


Nella finestra che compare, inserire la password che servirà per accedere al file.

La password non deve contenere dati personali.



Nella finestra successiva inserire nuovamente la stessa password per confermare il precedente inserimento.



N.B. Conservare la password in un luogo sicuro, per esempio **non** in una chiavetta USB.

N.B. Dopo aver impostato la password per la crittografia, anche il proprietario del file dovrà inserirla ogni volta che apre il file.

4. Togliere la crittografia a un file in Office 365

Per togliere la crittografia a un file bisogna ripetere la stessa procedura lasciando vuoto il campo della password.

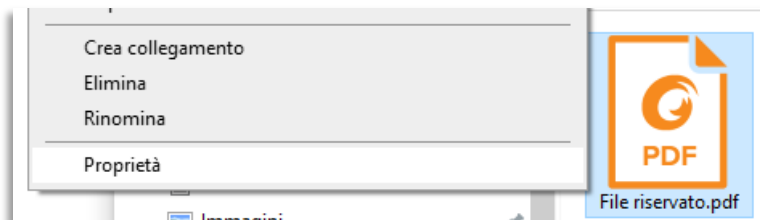
N.B. Se si dimentica la password di accesso a un file, non sarà possibile disattivarne la crittografia.

5. Crittografare un file su Windows 10

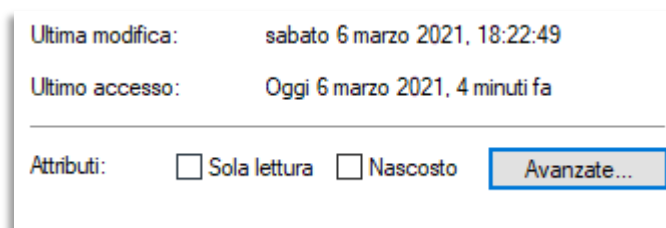
È possibile crittografare qualsiasi tipo di file utilizzando una funzionalità integrata in Windows 10, esclusa la versione Home.

Per crittografare un file seguire la seguente procedura, qui mostrata per un file pdf.

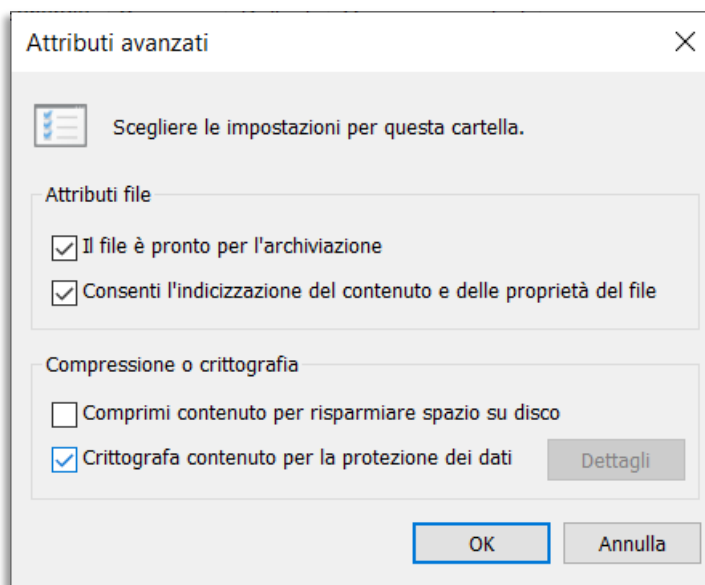
Cliccare con il tasto destro sul file e selezionare Proprietà.



Nella finestra che si apre, cliccare su Avanzate.



Nella finestra che si apre, spuntare “Crittografa contenuto per la protezione dei dati” e confermare con OK in entrambe le finestre.



N.B. Chi utilizza altri sistemi operativi è invitato a crittografare i file tramite Office 365 e a salvarli in pdf e inviarli tramite l'e-mail istituzionale; i sistemi operativi macOS dispongono di una funzionalità integrata di crittografia per i file, si veda ad es. il sito del supporto di Apple alla pagina <https://support.apple.com/it-it/guide/mac-help/mh40593/11.0/mac/11.0>. In alternativa si possono usare programmi specifici che permettono di crittografare singoli file, cartelle o anche interi dispositivi.