

## **Istituto d'Istruzione Superiore Faicchio con sede coordinata di Castelvenere**

Istituto Tecnico per il Turismo

Istituto Professionale Servizi Socio Sanitari – Odontotecnico

Istituto Professionale Servizi per l'Enogastronomia e l'Ospitalità Alberghiera

Corso Serale **IPSEOA** Castelvenere

Corso Serale **Servizi Socio- Sanitari** Faicchio

Faicchio: Via Raffaele Delcogliano e Aldo Iermano cap. 82030 tel. +39 0824863478

Castelvenere: Piazza dei Caduti, cap. 82037 tel. +39 0824940154

Codice fiscale: 90003320620 - Codice meccanografico: **BNIS02300V** - Codice unico di fatturazione (CUF): UFGEG8

Email: [bnis02300v@istruzione.it](mailto:bnis02300v@istruzione.it) - Posta elettronica certificata (PEC): [bnis02300v@pec.istruzione.it](mailto:bnis02300v@pec.istruzione.it)

<https://www.iisfaicchio-castelvenere.edu.it>

RETE DI FORMAZIONE AMBITO BN05  
Formazione docenti D.M. 732 Piano Nazionale per la Formazione

Circ. n. 34

Faicchio, 09/10/2024

Al sito WEB:

[www.iisfaicchio-castelvenere.edu.it](http://www.iisfaicchio-castelvenere.edu.it)

AI DOCENTI

AGLI STUDENTI E ALLA STUDENTESSE

AL DSGA

AL PERSONALE ATA

**OGGETTO:** Corretto utilizzo dei dispositivi elettronici scolastici

### **Diritti e responsabilità dei dipendenti**

Per assicurare la tutela dei diritti, delle libertà fondamentali e della dignità dei lavoratori, per proteggere la riservatezza nelle relazioni personali professionali, ogni utente è responsabile, sotto il profilo **sia civile sia penale**, del corretto uso delle Risorse informatiche, dei Servizi e dei programmi ai quali ha accesso e dei dati che tratta. Spetta ai docenti vigilare affinché gli studenti loro affidati rispettino il presente regolamento.

### **Doveri di comportamento dei dipendenti**

Le strumentazioni informatiche, la rete Internet e la posta elettronica devono essere utilizzati dal personale e dagli studenti **unicamente come strumenti di lavoro e studio**. Ogni loro utilizzo non inerente all'attività lavorativa e di studio è vietato, in quanto può comportare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. In particolare non può essere dislocato nelle aree di condivisione della rete alcun file che non sia legato all'attività lavorativa, nemmeno per brevi periodi. Agli utenti è assolutamente vietata la memorizzazione di documenti informatici di natura oltraggiosa o discriminatoria per sesso lingua religione, razza, origine etnica, condizioni di salute, opinioni appartenenza sindacale politica.

Non è consentito scaricare, scambiare o utilizzare materiale coperto dal diritto d'autore.

## Elenco programmi ufficiali da usare nell' istituto Faicchio-Castelvenere

Gli unici software consentiti sono riportati nel seguente elenco:

- **SISTEMA OPERATIVO MICROSOFT WINDOWS 10 - 11**
- **ACROBAT READER**
- **WINRAR**
- **CROME**
- **EDGE**
- **PROGRAMMI UFFICIALI DEI LIBRI**
- **ANTIVIRUS USARE QUELLO DI DEFAULT MICROSOFT SICUREZZA WINDOWS**
- **PACCHETTO LIBRA OFFICE FREE CHE SOSTITUISCE MICROSOFT OFFICE .**

Non è consentito installare software diversi da quelli ufficiali, in dotazione alla scuola  
È altresì vietata la visualizzazione di film e di trasmissioni varie in streaming.

### Utilizzo dei personal computer

Gli utenti utilizzano per il proprio lavoro soltanto computer di proprietà dell'istituto, salvo espresse autorizzazioni contrarie dell'Amministratore di sistema/rete, e sono tenuti a:

- non inserire password locali che non rendano accessibile il computer agli amministratori di rete se non esplicitamente autorizzato dall'Amministratore di Sistema;
- non utilizzare cripto-sistemi o qualsiasi altro programma di sicurezza crittografia non previste esplicitamente dal servizio informatico dell'istituto;
- non modificare la configurazione hardware e software del proprio PC, se non esplicitamente autorizzati dall'Amministratore di Sistema;
- non rimuovere, danneggiare o asportare componenti hardware;
- non installare autonomamente programmi informatici, se non esplicitamente autorizzati dall'Amministratore di Sistema;
- non utilizzare programmi non autorizzati, con particolare riferimento ai videogiochi, che sono spesso utilizzati per veicolare virus;
- mantenere sempre aggiornati e attivi sulla propria postazione di lavoro i software antivirus con riferimento all'ultima versione disponibile;
- qualora il software antivirus rilevi la presenza di un virus, sospendere immediatamente ogni elaborazione in corso senza spegnere il computer e segnalare prontamente l'accaduto al personale incaricato dell'assistenza tecnica;
- prestare la massima attenzione ai supporti di origine esterna (es. pen - drive), verificando preventivamente tramite il programma di antivirus ogni file acquisito attraverso qualsiasi supporto e avvertendo immediatamente l'Amministratore di Sistema nel caso in cui vengano rilevati virus o eventuali malfunzionamenti;
- non lasciare incustodita ed accessibile la propria postazione una volta connesso al sistema con le proprie credenziali di autenticazione;
- non cedere, una volta superata la fase di autenticazione, l'uso della propria stazione a persone non autorizzate, in particolar modo per quanto riguarda l'accesso a Internet e ai servizi di posta elettronica;
- spegnere il PC al termine del lavoro o in caso di assenze prolungate dalla propria postazione.

**Il Dirigente Scolastico**

**Prof.ssa Maria Ester Riccitelli**

Firma autografa sostituita da indicazioni a mezzo stampa,  
ai sensi dell'art. 3 comma 2, D.Lgs. n. 39/1993