

Istituto Comprensivo di Traona

Costiera dei Cech



Ministero dell'Istruzione

ISTITUTO COMPRENSIVO DI TRAONA

Via Aldo Moro n. 6 - 23019 TRAONA (SO) - Tel. 0342 653340

Codice Fiscale: 82003850144 - Codice Ufficio Univoco UFZVHU

e-mail: SOIC81200L@ISTRUZIONE.IT - SOIC81200L@PEC.ISTRUZIONE.IT

sito web: www.ictraona.edu.it

E-policy

Regole e consigli per l'uso delle nuove tecnologie

INTRODUZIONE

L'uso delle nuove tecnologie ha contribuito in maniera decisiva a ridefinire lo spazio pubblico e privato, a strutturare i rapporti tra le persone e tra queste e le Istituzioni. Ha cancellato confini e ha costruito modalità nuove di produzione e utilizzazione della conoscenza. Ha ampliato le possibilità di intervento diretto delle persone nella sfera pubblica. Ha modificato l'organizzazione del lavoro. Ha consentito lo sviluppo di una società più aperta e libera.

Tutto ciò non può essere ignorato dal mondo della scuola, che, oltre a dover fare suo questo spazio per relazionarsi meglio con gli studenti e offrire una didattica più efficace, deve anche guidarli nell'approfondire e padroneggiare in modo sicuro, consapevole e responsabile gli strumenti informatici. *(tratto con leggere modifiche dalla Dichiarazione dei diritti in Internet elaborato dalla Commissione per i diritti e i doveri in Internet della Camera dei Deputati 28 luglio 2015)*

In tale ottica l'Istituto comprensivo di Traona ha attivato la piattaforma di e-learning Google Suite for Education (GSfE), partecipato ad azioni di formazione del personale all'interno del Piano Nazionale Scuola Digitale (PNSD) e ha intenzione di programmare delle azioni di formazione rivolte a famiglie e studenti.

In continuità con queste azioni, la scuola ha predisposto il presente documento (E-Policy), rivolto ad alunni, genitori e insegnanti, pensato per definire misure atte a facilitare e promuovere l'utilizzo delle TIC e nello stesso tempo stabilire norme comportamentali e procedure per l'utilizzo delle stesse, in particolare nell'ambito dell'Istituto.

Nella parte finale sono presentati i principali Pericoli nell'uso delle TIC, non con lo scopo di allontanare le persone dal web o dall'uso dei social media, ma con l'obiettivo di aiutare i genitori e gli insegnanti ad educare i ragazzi ad avvicinarsi ad internet nel modo corretto.

CONDIVISIONE, MONITORAGGIO E AGGIORNAMENTO DELL'E-SAFETY

Questo documento è fatto oggetto di condivisione attraverso l'approvazione da parte del Collegio dei Docenti e del Consiglio di Istituto, la sua applicazione viene monitorata dal Team per l'innovazione digitale che ne cura anche eventuali aggiornamenti.

LA COMPETENZA DIGITALE

La Raccomandazione del Consiglio europeo del 22 maggio 2018 relativa alle competenze chiave per l'apprendimento permanente (2018/C 189/01) individua le 8 competenze chiave per l'apprendimento permanente, definendo tra queste la competenza digitale:

La competenza digitale presuppone l'interesse per le tecnologie digitali e il loro utilizzo con dimestichezza e spirito critico e responsabile per apprendere, lavorare e partecipare alla società.

Essa comprende l'alfabetizzazione informatica e digitale, la comunicazione e la collaborazione, l'alfabetizzazione mediatica, la creazione di contenuti digitali (inclusa la programmazione), la sicurezza (compreso l'essere a proprio agio nel mondo digitale e possedere competenze relative alla cybersicurezza), le questioni legate alla proprietà intellettuale, la risoluzione di problemi e il pensiero critico.

Conoscenze, abilità e atteggiamenti essenziali legati a tale competenza

Le persone dovrebbero comprendere in che modo le tecnologie digitali possono essere di aiuto alla comunicazione, alla creatività e all'innovazione, pur nella consapevolezza di quanto ne consegue in termini di opportunità, limiti, effetti e rischi. Dovrebbero comprendere i principi generali, i meccanismi e la logica che sottendono alle tecnologie digitali in evoluzione, oltre a conoscere il funzionamento e l'utilizzo di base di diversi dispositivi, software e reti.

Le persone dovrebbero assumere un approccio critico nei confronti della validità, dell'affidabilità e dell'impatto delle informazioni e dei dati resi disponibili con strumenti digitali ed essere consapevoli dei principi etici e legali chiamati in causa con l'utilizzo delle tecnologie digitali.

Le persone dovrebbero essere in grado di utilizzare le tecnologie digitali come ausilio per la cittadinanza attiva e l'inclusione sociale, la collaborazione con gli altri e la creatività nel raggiungimento di obiettivi personali, sociali o commerciali.

Le abilità comprendono la capacità di utilizzare, accedere a, filtrare, valutare, creare, programmare e condividere contenuti digitali. Le persone dovrebbero essere in grado di gestire e proteggere informazioni, contenuti, dati e identità digitali, oltre a riconoscere software, dispositivi, intelligenza artificiale o robot e interagire efficacemente con essi.

Interagire con tecnologie e contenuti digitali presuppone un atteggiamento riflessivo e critico, ma anche improntato alla curiosità, aperto e interessato al futuro della loro evoluzione. Impone anche un approccio etico, sicuro e responsabile all'utilizzo di tali strumenti.

Ruolo degli insegnanti

Il docente può avvalersi della strumentazione TIC della scuola o di tablet, smartphone e computer portatili personali rispettando quanto stabilito dal presente documento.

Nell'ambito delle scelte educative e didattiche compiute per portare i propri alunni a conseguire la competenza digitale, il docente deve anche:

- ❖ *illustrare ai propri alunni le regole stabilite dall'E-safety della scuola;*
- ❖ *guidare gli alunni ad un corretto accesso alle TIC, condividendo con gli alunni la **netiquette**, aiutandoli a comprendere i **principali rischi** ed illustrando le **linee guida**;*
- ❖ *garantire che le comunicazioni digitali dei docenti con alunni e genitori siano svolte nel rispetto del codice di comportamento professionale ed effettuate con sistemi scolastici ufficiali (posta elettronica istituzionale e registro elettronico);*
- ❖ *comunicare ai genitori difficoltà, bisogni o disagi espressi dagli alunni (ovvero valutazioni sulla condotta non adeguata degli stessi) connessi all'utilizzo delle TIC, al fine di approfondire e concordare coerenti linee di intervento.*

Infine, pur non volendo in nessun modo invadere le legittime scelte dei docenti nella loro vita fuori dal contesto scolastico, si suggerisce di evitare comportamenti esasperati sui social network e registri comunicativi poco affini al ruolo ricoperto in ambito educativo;

Ruolo degli alunni

Essendo la competenza digitale una delle otto competenze chiave per l'apprendimento permanente, ogni alunno ha il dovere, oltre che il diritto, di attivarsi per migliorare le proprie conoscenze e abilità nell'uso delle TIC e nel farlo deve anche:

- ❖ *utilizzare in modo responsabile, in relazione al proprio grado di maturità e di apprendimento, i sistemi delle tecnologie digitali in conformità con quanto richiesto dai docenti;*
- ❖ *avere una buona comprensione delle potenzialità offerte dalle TIC per la ricerca di contenuti e materiali ma anche della necessità di evitare il plagio e rispettare i diritti d'autore;*
- ❖ *comprendere l'importanza di adottare buone pratiche di sicurezza on-line quando si utilizzano le tecnologie digitali;*
- ❖ *adottare condotte rispettose degli altri anche quando comunica in rete;*

- ❖ esprimere domande o difficoltà o bisogno di aiuto nell'utilizzo delle tecnologie didattiche o di internet ai docenti e ai genitori.

Ruolo dei genitori

L'uso delle TIC offre grandi opportunità, ma comporta rischi, i genitori devono esserne consapevoli, ma non per questo dovrebbero impedirne l'accesso ai propri figli.

I genitori sono chiamati a sostenere la linea di condotta della scuola adottata nei confronti dell'utilizzo delle TIC nella didattica, prendendo visione del presente documento e condividendolo con i propri figli.

GESTIONE DELL'INFRASTRUTTURA E DELLA STRUMENTAZIONE ICT DELLA SCUOLA

Strumentazione dei Laboratori e delle aule

I docenti sono liberi di utilizzare la strumentazione presente nelle aule (LIM e computer) e nei laboratori (Videoproiettori e computer e stampanti) per organizzare le lezioni, per l'accesso al registro elettronico, per la formazione o per questioni amministrative osservando le seguenti indicazioni:

- ❖ rispettare e far rispettare gli eventuali regolamenti previsti per i laboratori di informatica, l'aula musica, l'aula magna e la biblioteca;
- ❖ non installare software senza prima aver chiesto il permesso al responsabile dell'area informatica e comunque non farlo senza le dovute licenze d'uso;
- ❖ assumersi la responsabilità di segnalare prontamente eventuali malfunzionamenti o danneggiamenti al responsabile informatico;
- ❖ non allontanarsi dalla postazione lasciandola incustodita, se non prima di aver effettuato la disconnessione;
- ❖ non divulgare le credenziali di accesso agli account (username e password) o alla rete wifi;
- ❖ non salvare sulle postazioni utilizzate file contenenti dati personali o sensibili;

Gli alunni possono utilizzare la strumentazione presente nelle aule e nei laboratori solo con il permesso di un docente e in sua presenza o di altro personale incaricato della sorveglianza, osservando le seguenti indicazioni:

- ❖ rispettare i regolamenti previsti per i laboratori di informatica, l'aula musica, l'aula magna e la biblioteca;
- ❖ avere cura della strumentazione e segnalare prontamente eventuali malfunzionamenti o danneggiamenti al docente presente;
- ❖ aver cura di spegnere in modo corretto i computer e i monitor al termine del loro utilizzo, a meno di diverse disposizioni da parte del docente;

Strumentazione dell'aula insegnanti

Solo al personale della scuola è consentito accedere alle postazioni informatiche presenti in aula insegnanti, a meno di un'autorizzazione fornita dal responsabile informatico, dal Responsabile di plesso o dal Dirigente scolastico.

Il personale della scuola può utilizzare la strumentazione solo per motivi didattici o professionali, osservando le seguenti indicazioni:

- ❖ assumersi la responsabilità di segnalare prontamente eventuali malfunzionamenti o danneggiamenti al responsabile informatico;
- ❖ non installare software senza prima aver chiesto il permesso al responsabile dell'area informatica e comunque non farlo senza le dovute licenze d'uso;
- ❖ non allontanarsi dalla postazione lasciandola incustodita, se non prima di aver effettuato la disconnessione;
- ❖ non divulgare le credenziali di accesso agli account (username e password) o alla rete wifi;

- ❖ *non salvare sulle postazioni utilizzate file contenenti dati personali o sensibili;*
- ❖ *limitarsi a stampare ciò che è necessario e selezionare i dispositivi di stampa a colori solo quando è utile.*

STRUMENTAZIONE PERSONALE

L'istituto comprensivo di Traona è aperto al BYOD (bring your own device), ma richiede che vengano rispettate alcune regole.

Personale scolastico

Nell'orario di servizio al personale scolastico è consentito l'utilizzo di smartphone, tablet e computer portatili solo a scopo didattico o per attività amministrative ad integrazione degli strumenti scolastici disponibili.

Alunni

Durante l'orario scolastico è consentito l'uso di telefoni cellulari, tablet o computer portatili solo con l'autorizzazione ed il controllo da parte degli insegnanti e solo per motivi didattici.

In nessun caso potranno essere scattate foto, registrati video o audio senza il permesso dei docenti e comunque nel rispetto di quanto contenuto in questo documento.

I predetti dispositivi dovranno essere tenuti spenti nei momenti di inutilizzo e, nel caso degli smartphone, depositati nell'apposito contenitore presente in tutte le classi. Lo stesso contenitore non dovrà mai essere lasciato incustodito nella classe senza prima chiudere la porta a chiave.

Eventuali esigenze di comunicazione tra gli alunni e le famiglie, in caso di urgenza, potranno essere soddisfatte mediante il telefono della scuola;

ACCESSO ALLA RETE DELL'ISTITUTO

La rete dell'istituto è a disposizione del personale e degli studenti per finalità didattiche, di formazione o amministrative.

In considerazione che la larghezza della banda per il traffico dei dati non è illimitato, ognuno è tenuto ad un comportamento che rispetti anche le esigenze degli altri utilizzatori.

E' possibile accedere alla rete di istituto in due modalità: come utente riconosciuto o come ospite.

In entrambi i casi deve risultare possibile identificare l'autore della connessione.

Utente riconosciuto

Questo tipo di accesso si ha attraverso tutti i dispositivi di proprietà della scuola

Ospite

Questo tipo di accesso è concesso ai dispositivi dei docenti (massimo uno) e degli studenti per attività didattiche. I docenti avranno cura di procurarsi le credenziali dal responsabile informatico e, se dovessero servire per gli studenti, di consegnarle registrando l'accoppiamento dispositivo-username;

ACCESSO AD INTERNET

Internet è un elemento importante nella didattica del XXI secolo, ma considerando che vi compaiono anche contenuti non adeguati a dei minori è necessario un accesso regolamentato.

Personale scolastico

Il personale scolastico può utilizzare la rete dell'istituto per accedere ad internet solo per motivi didattici, di formazione o amministrativi.

Nelle lezioni in cui è programmato l'utilizzo di Internet i docenti devono guidare gli alunni a siti controllati e ritenuti adatti alla loro età e verificare che nelle ricerche su Internet siano trattati solo materiali idonei.

In particolare i docenti devono porre attenzione nell'uso del registro elettronico e della piattaforma Google Suite for Education, evitando di lasciare la postazione a disposizione di altri utenti quando è aperta una sessione con uno di questi due applicativi.

Alunni

Gli alunni possono utilizzare la rete dell'istituto per accedere ad internet solo con l'autorizzazione e la presenza di un docente e comunque rispettando le indicazioni contenute in questo documento.

Particolare attenzione deve essere posta nell'uso di Google Suite for Education, ricordandosi di effettuare la disconnessione al termine della sessione di lavoro ed evitando di divulgare la propria password.

NETIQUETTE

Fra gli utenti di Internet si sono sviluppate, nel corso del tempo, una serie di tradizioni e di norme di buon senso che costituiscono la "Netiquette" (Galateo della Rete).

Nella comunicazione interpersonale (posta elettronica, chat, forum ecc.) è importante:

- ❖ sentirsi liberi di esprimere le proprie idee, nei limiti dell'educazione e del rispetto altrui: ben vengano le discussioni vivaci ed animate, ma senza trascendere i suddetti limiti;
- ❖ evitare messaggi con insulti o parolacce;
- ❖ non inviare mai lettere a catena via posta elettronica. Su Internet le lettere a catena sono vietate, pena la revoca dell'account;
- ❖ evitare di inoltrare ad altri le conversazioni private;
- ❖ non inviare tramite posta elettronica messaggi pubblicitari o comunicazioni che non siano state richieste;
- ❖ evitare di scrivere i messaggi in caratteri maiuscoli: equivale ad URLARE;
- ❖ non essere intolleranti con chi commette errori sintattici o grammaticali. Chi scrive, è comunque tenuto a migliorare il proprio linguaggio in modo da risultare comprensibile alla collettività;
- ❖ valutare che nella forma scritta il linguaggio gestuale e il tono di voce vengono a mancare e questo può portare a fraintendimenti. Spesso per ovviare a questo problema si utilizzano gli smiles (faccine). E' bene però non eccedere anche in considerazione del livello di formalità della comunicazione.

Infine: lo spazio virtuale (internet e social media) non sono una "zona franca" dove le leggi sono sospese. Chi invia o pubblica messaggi offensivi può essere perseguito per reati quali diffamazione, oltraggio o calunnia, aggravati dalla diffusione indiscriminata.

L'utente è sempre individuabile dalle autorità attraverso l'indirizzo di rete unico (IP) del computer, anche quando non utilizza il proprio nome.

PRINCIPALI RISCHI CONNESSI ALL'USO DELLE TIC

Per tantissimi adulti e ragazzi l'uso della tecnologia in modo sistematico è la normalità, tuttavia non sempre colgono le implicazioni dei loro comportamenti e questo avviene ancor più facilmente al diminuire dell'età. Non sempre i pericoli vengano percepiti come tali. Di seguito vengono riportati i principali, ricordando che è compito degli adulti, docenti e genitori, guidare i ragazzi a saperli riconoscere ed evitare.

- ❖ *esposizione a contenuti violenti o non adatti alla loro età;*
- ❖ *diffusione in rete di dati personali;*
- ❖ *videogiochi diseducativi;*
- ❖ *pubblicità ingannevoli;*
- ❖ *informazioni scorrette;*
- ❖ *virus informatici in grado di infettare computer e cellulari;*
- ❖ *furto di identità o di credenziali informatiche;*
- ❖ *possibili contatti con adulti che vogliono conoscere e avvicinare bambini/e o ragazzi/e (adescamento);*
- ❖ *rischio di molestie o maltrattamenti da coetanei (cyber-bullismo);*
- ❖ *scambio di materiale a sfondo sessuale (sexting);*
- ❖ *uso eccessivo di Internet/cellulare (dipendenza).*

LINEE GUIDA PER GLI ALUNNI

- ❖ *Non comunicare mai a nessuno la tua password e cambiala periodicamente, usando numeri, lettere e caratteri speciali;*
- ❖ *non divulgare sulla rete i tuoi dati personali quali indirizzi e numeri di telefono;*
- ❖ *prima di inviare ad altri o pubblicare in uno spazio pubblico una fotografia tua o di qualcun altro, chiedi sempre il permesso agli adulti di riferimento (genitori o insegnanti);*
- ❖ *chiedi sempre al tuo insegnante a scuola o ai tuoi genitori a casa il permesso di scaricare file da Internet;*
- ❖ *chiedi sempre il permesso ai tuoi genitori prima di iscriverti a qualche sito o concorso;*
- ❖ *quando sei connessi alla rete rispetta sempre gli altri, ciò che per te è un gioco può rivelarsi offensivo per qualcun altro;*
- ❖ *non rispondere alle offese ed agli insulti;*
- ❖ *conserva le comunicazioni offensive, ti potrebbero essere utili per dimostrare quanto ti è accaduto;*
- ❖ *se ricevi materiale offensivo (email, sms, mms, video, foto, messaggi vocali) non diffonderlo: potresti essere accusato di cyberbullismo;*
- ❖ *rifletti prima di inviare commenti o documenti: ricordati che tutto ciò che invii su internet diviene pubblico ed è quasi impossibile eliminarlo;*
- ❖ *riferisci al tuo insegnante o ai tuoi genitori se qualcuno ti invia immagini che ti infastidiscono e non rispondere;*
- ❖ *se qualcuno su Internet ti chiede un incontro di persona, riferiscilo al tuo insegnante o ai tuoi genitori;*
- ❖ *ricordati che le persone che incontri nella Rete sono degli estranei e non sempre sono quello che dicono di essere;*
- ❖ *tutti gli studenti della secondaria sono in possesso di un account GSfE gestito dalla scuola, puoi utilizzarlo solo per inviare mail ai tuoi compagni e ai docenti.*

CONSIGLI AI GENITORI PER UN USO RESPONSABILE DI INTERNET A CASA

- ❖ *Se possibile, posizionate il computer utilizzato da vostro figlio in una stanza accessibile a tutta la famiglia;*
- ❖ *evitate di lasciare le e-mail o file personali sui computer di uso comune;*
- ❖ *concordate con vostro figlio le regole: quando si può usare internet e per quanto tempo. Vostro figlio potrebbe dirvi che il suo migliore amico ha la possibilità di navigare tutti i giorni a tutte le ore...che fare? se è possibile create una partnership con i genitori dei migliori amici di vostro figlio in modo da concordare con loro le regole: tempi di connessione, fasce orarie e siti autorizzati;*
- ❖ *inserite nel computer i filtri di protezione: prevenite lo spam, i pop-up pubblicitari, l'accesso a siti pornografici;*
- ❖ *utilizzate il filtro del "parental control" attraverso la sezione sicurezza in internet dal pannello di controllo (è possibile farlo anche sugli smartphones);*
- ❖ *attivate firewall (protezione contro malware) e antivirus;*
- ❖ *sentitevi coinvolti: chiedete a vostro figlio di mostrarvi come funziona internet e come viene usato per scaricare e caricare compiti, lezioni, materiali didattici e per comunicare con l'insegnante;*
- ❖ *incoraggiate le attività on line di alta qualità: ricercare informazioni scientifiche, documentarsi, studiare o svolgere compiti;*
- ❖ *spiegate a vostro figlio che le password, i codici pin, i numeri di carta di credito e i numeri di telefono e i dettagli degli indirizzi e-mail sono privati e non devono essere dati ad alcuno;*
- ❖ *chiarite a vostro figlio ciò che ritenete inaccettabile (razzismo, violenza, linguaggio volgare, pornografia);*
- ❖ *discutete sulla necessità di porre attenzione nello scaricare e caricare file sulla rete;*
- ❖ *incoraggiate vostro figlio a dirvi se vede immagini particolari o se riceve messaggi indesiderati;*
- ❖ *discutete nei dettagli le conseguenze che potranno esserci se vostro figlio visita deliberatamente siti non adatti, ma non rimproveratelo se compie azioni involontarie;*
- ❖ *spiegate a vostro figlio che non tutti in Internet sono realmente chi dichiarano di essere.*

INDIRIZZI UTILI

Di seguito vengono riportati i riferimenti ad alcuni siti che possono risultare utili per approfondire e gestire situazioni problematiche relative alle tematiche trattate in questo documento.

Compartimento Polizia postale Lombardia –Sezione Sondrio

Per comunicare qualsiasi cosa che si ritenga sospetta, di cattivo gusto, pericolosa o altro mentre si sta navigando in Internet, ed avere un aiuto concreto:

Telefono: 0342545527 (sede di Sondrio)

e-mail: compartimento.polposta.mi@pecps.poliziadistato.it (sede di Milano)

Sportello Cyberbullismo

Lo sportello Cyberbullismo è un servizio promosso dal CTS (centro Supporto Territoriale) che ha la propria sede presso il Liceo "G. Piazzi – C. Lena Perpentì" a Sondrio, in via Tonale presso il Campus Scolastico. Per contattare gli operatori:

e-mail: sportellocyberbullismo@piazzenaperpentì.it

info@sondriocets.it

telefono: 0342-211766 (centralino del Liceo Piazzi Lena Perpentì)

con hangout accedendo attraverso questo link ed utilizzando il seguente identificativo:

sportellocyberbullismo@piazzenaperpentì.it

Co.re.com Lombardia "Sportello help web reputation giovani"

Il Comitato regionale per le comunicazioni della Lombardia ha dato vita allo Sportello Help Web Reputation Giovani, un servizio totalmente gratuito rivolto ai cittadini lombardi (esclusivamente persone fisiche) che riscontrano problemi in merito alla propria reputazione digitale. Scopo dello sportello è quello di aiutare concretamente gli utenti della "Rete" nella tutela della propria web reputation.

Sito web: www.corecomlombardia.it

e-mail: sportellowebreputation@consiglio.regione.lombardia.it

Telefono 02 67482725

Generazioni Connesse

Il progetto "Generazioni connesse". gestito dal MIUR, mette a disposizione:

due servizi di Hotlines (www.azzurro.it e www.stop-it.it), che consentono agli utenti di segnalare la presenza di materiale illegale, in particolare pedopornografico trovato online;

la Helpline di Telefono Azzurro a sostegno del Progetto (telefono 1.96.96) – servizio in grado di fornire supporto, in particolare a bambini, adolescenti e genitori in merito a esperienze negative e/o problematiche inerenti l'utilizzo di Internet e tecnologie digitali.