Ministero dell'Istruzione
ISTITUTO TECNICO STATALE F. VIGANÒ
Via Dei Lodovichi, 2 – 23807 Merate LC
Codice Fiscale: 85002000132 – Codice Univoco:UFSL80
Tel: 0399902998 - 0399907117 - Fax: 0399908965
segreteria@issvigano.edu.it– lcis001009@pec.istruzione.it
www.issvigano.edu.it

E-POLICY

Il documento di e-Policy rappresenta un documento autoprodotto dalla scuola che serve a promuovere un uso positivo delle nuove tecnologie al fine di riconoscere, prevenire e rispondere a possibili situazioni problematiche.
Nel documento viene descritto l'approccio con cui la scuola si rivolge alle tematiche legate alle competenze digitali, alla sicurezza online e ad un uso positivo delle tecnologie digitali nella didattica; vengono inoltre indicate le norme comportamentali e le procedure per l'utilizzo delle Tecnologie dell'informazione e della comunicazione (TIC) in ambiente scolastico, le misure per la prevenzione e le misure per la rilevazione e gestione delle problematiche connesse ad un uso non consapevole delle tecnologie digitali.

1. INTRODUZIONE
   - Scopo della Policy
   - Ruoli e responsabilità dei componenti della Comunità Scolastica
   - Condivisione e comunicazione della Policy all'intera comunità scolastica
   - Gestione delle infrazioni alla Policy
   - Monitoraggio dell'implementazione alla Policy e suo aggiornamento
   - Integrazione della Policy con regolamenti esistenti
2. FORMAZIONE E CURRICOLO
   - Curricolo delle competenze digitali per gli studenti
   - Formazione dei docenti
   - Sensibilizzazione delle famiglie
3. INFRASTRUTTURA E STRUMENTAZIONE TIC (O ICT)
   - Accesso a Internet: filtri antivirus e sulla navigazione
   - Gestione accessi: password, backup, ect..
   - E-mail
   - Blog e sito web della scuola
   - Social network
   - Protezione dati personali
4. DISPOSITIVI PERSONALI
   - Per gli studenti: gestione degli strumenti personali (cellulari, tablet, ect…)
   - Per i docenti : gestione degli strumenti personali (cellulari, tablet, ect…)
   - Per il personale della scuola: gestione degli strumenti personali (cellulari, tablet, ect…)
5. PREVENZIONE, RILEVAZIONE, GESTIONE CASI
   - Prevenzione : rischi/azioni
   - Rilevazione : cosa segnalare, come segnalare (quali strumenti e a chi), come gestire le segnalazioni
   - Gestione dei casi: definizione delle azioni da intraprendere a secondo del caso
6. ALLEGATI

1.INTRODUZIONE

Il nostro Istituto si è dimostrato attivo nello studio, analisi e confronto di tematiche e rischi legati all'uso delle nuove tecnologie: la partecipazione a corsi di perfezionamento, la partecipazione ad incontri di formazione, incontri con i genitori degli alunni, l'emanazione di norme interne riguardo l'uso ed abuso dei dispositivi informatici (Regolamento di istituto, il Patto di corresponsabilità sottoscritto da genitori e studenti), informativa sul trattamento dei dati personali (ai sensi dell'art. 13 del D. Lgs. 30 giugno 2003, n. 196) e richiesta di autorizzazione all'utilizzo dei dati personali degli alunni eccedenti i trattamenti istituzionali obbligatori, come per esempio l'utilizzo di fotografie, video o altri materiali audiovisivi contenenti l'immagine, il nome e/o la voce del proprio figlio/a, all'interno di attività educative e didattiche per scopi documentativi, formativi e informativi, durante gli anni di frequenza della scuola.
All'inizio dell'anno scolastico viene letto il regolamento d'Istituto ai ragazzi e viene pubblicata una circolare in cui si invitano le famiglie e tutto il personale scolastico a prendere visione dello stesso.
La redazione del presente documento nasce dalla necessità di dare concretezza alle "Linee di orientamento" per la prevenzione e il contrasto del cyberbullismo che danno continuità alle Linee guida elaborate dal gruppo di lavoro istituito con Decreto Dipartimentale n. 1140 del 30 ottobre 2015 tenendo conto delle novità contenute nella L.71/2017 "Disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del cyberbullismo".

SCOPO
Lo scopo che ci si propone in questa sede è, dunque, quello di descrivere l'approccio dell'Istituto alle tematiche legate alle competenze digitali, all'uso degli stessi in ambiente scolastico ed alla sicurezza in rete in termini di:

- individuazione di norme comportamentali e delle procedure per l'utilizzo delle Tecnologie dell'Informazione e della Comunicazione (TIC);
- promozione dell'uso positivo delle tecnologie digitali nella didattica;
- adozione delle misure per la prevenzione del fenomeno del cyberbullismo e,contestualmente, individuazione degli strumenti di tutela per chi risultasse vittima dicomportamenti (anche solo potenzialmente) vessatori e di emarginazioneattraverso un uso distorto e violento della rete;
- sensibilizzazione degli studenti orientandoli verso un uso corretto delle tecnologiedigitali.

Il tutto in coerenza con lo spirito della Legge 71/2017 che è quello di un approccio sostanzialmente inclusivo con interventi dalla finalità educativa e mai punitiva.
Il presente documento sarà soggetto a revisioni ed aggiornamenti periodici e sottoposto all'attenzione dei competenti Organi Collegiali.

RUOLI E RESPONSABILITA' (cosa ci si aspetta da tutti i componenti della Comunità Scolastica)

IL DIRIGENTE SCOLASTICO

- Responsabilità generale per i dati e la sicurezza dei dati
- Garantire che la scuola utilizzi un Internet Service filtrato approvato, conforme ai requisiti di legge vigenti
- La responsabilità che il personale riceva una formazione adeguata per svolgere i ruoli di sicurezza on-line e per la formazione di altri colleghi
- Essere a conoscenza delle procedure da seguire in caso di infrazione della E-Safety Policy
- Ricevere relazioni di monitoraggio periodiche della sicurezza on-line da parte del responsabile
- Garantire che vi sia un sistema in grado di monitorare il personale di supporto che svolge le procedure di sicurezza on-line interne

I RESPONSABILI DELLA SICUREZZA ONLINE (DSGA E DOCENTI SU NOMINA DEL DS)

- Responsabilità per i problemi di sicurezza on-line
- Promuovere la consapevolezza e l'impegno per la salvaguardia online in tutta la comunità scolastica
- Garantire che tutto il personale sia a conoscenza delle procedure che devono garantire la sicurezza online
- Facilitare la formazione e la consulenza per tutto il personale
- Coordinarsi con le autorità locali e le agenzie competenti
- Controllare la condivisione dei dati personali
- Controllare l'accesso a materiali illegali/inadeguati
- Controllare probabili azioni di cyber bullismo

ANIMATORE DIGITALE E SUO TEAM

- Pubblicare la E-Safety Policy sul sito della scuola
- Diffusione della E-Safety Policy attraverso power point e schede semplificative
- Garantire che tutti i dati relativi agli alunni siano sufficientemente tutelati

DOCENTI

- Inserire tematiche legate alla sicurezza online nel programma di studi
- Supervisionare e guidare gli alunni con cura quando sono impegnati in attività di apprendimento che coinvolgono la tecnologia online
- Garantire che gli alunni siano pienamente consapevoli dei problemi relativi ai contenuti elettronici

IL PERSONALE SCOLASTICO

- Comprendere e promuovere politiche di e-sicurezza
- Essere consapevoli di problemi di sicurezza online connessi con l'uso di telefoni cellulari, fotocamere, dispositivi portatili
- Monitorare l'uso di dispositivi tecnologici e attuare politiche scolastiche per quanto riguarda questi dispositivi
- Segnalare qualsiasi abuso sospetto o problema al responsabile della sicurezza online
- Usare comportamenti sicuri, responsabili e professionali nell'uso della tecnologia

GLI ALUNNI

- Leggere, comprendere e accettare la E-Safety Policy
- Capire l'importanza di segnalare abusi o l'uso improprio o l'accesso a materiali inappropriati
- Segnalare ai genitori e/o ai docenti situazioni di difficoltà o di bisogno di aiuto nell'utilizzo delle tecnologie digitali.
- Conoscere e capire la politica relativa all'uso dei cellulari, fotocamere digitali, dispositivi portatili
- Capire l'importanza di adottare buone pratiche di sicurezza online quando si usano le tecnologie digitali fuori dalla scuola
- Assumersi la responsabilità di conoscere i benefici e i rischi di utilizzo di internet e di altre tecnologie in modo sicuro e corretto, sia a scuola che a casa

I GENITORI

- Sostenere la scuola nel promuovere la sicurezza online e approvare l'accordo di E-Safety Policy con la scuola
- Leggere e comprendere il suddetto accordo
- Accedere al sito web della scuola in conformità con quanto stabilito dalla stessa
- Educare (vigilando sui propri figli) al corretto utilizzo delle tecnologie digitali inambiente domestico fissando regole comportamentali e di utilizzo
- Collaborare con i docenti nell'adozione di linee di intervento coerenti per contrastare l'uso non responsabile, scorretto o pericoloso delle tecnologie digitali.

CONDIVISIONE E COMUNICAZIONE DELLA POLICY ALL'INTERA COMUNITA' SCOLASTICA

La E- Safety Policy si applica a tutti i membri della scuola : personale, studenti, genitori
Il Dirigente Scolastico regola il comportamento degli studenti e autorizza i membri del personale di imporre sanzioni disciplinari in caso di comportamento inadeguato.
La Policy sarà comunicata al personale, agli alunni, alla comunità nei seguenti modi:

- pubblicazione della E-Safety Policy sul sito della scuola
- all'interno del Patto di Corresponsabilità, ai genitori verrà chiesto di leggere e di approvare l'accordo di e-Policy con la scuola che troveranno pubblicato sul sito istituzionale
- comunicazione della e-policy all'intera comunità scolastica attraverso la pubblicazione di una circolare

GESTIONE DELLE INFRAZIONI ALLA POLICY

Nell'ambito delle responsabilità del D.S.G.A., dell'animatore digitale e tutto il personale scolastico, si fa riferimento alle funzioni di responsabilità e controllo dirigenziale.
Il personale scolastico è tenuto a collaborare col D.S. per fornire ogni informazione utile per le valutazioni del caso e per l'avvio di eventuali procedimenti organizzativo gestionale,disciplinare, amministrativo, civile, penale, ecc.
I genitori collaborano con tutto il personale scolastico in quanto principali figure educative di riferimento dei propri figli.

Le principali operazioni relative al mancato rispetto della E-policy da parte degli alunni sono riconducibili a:

• uso di social network e blog per pubblicare, condividere o, in genere, postare commenti o giudizi offensivi della dignità altrui;
• condivisione di dati personali che possano permettere l'identificazione;
• connessioni a siti proibiti o comunque non autorizzati;
• pirateria informatica;
• scaricamento di file (video, film, musica, immagini, test, ecc.) per finalità personali;
• pubblicazione di foto o immagini non autorizzate e/o compromettenti.

Gli interventi previsti sono rapportati all'età, alla situazione personale, alla gravitàdell'operato. Si riporta di seguito un elenco non esaustivo di possibili azioni:
• richiamo verbale;
• richiamo verbale con annotazione disciplinare sul registro elettronico;
• prelievo del dispositivo e consegna in Vicepresidenza per il ritiro dello stesso da parte dei genitori;
• convocazione della famiglia e/o degli attori dell'episodio segnalato;
• raccolta del materiale informatico lesivo della dignità delle figure presenti nell'istituto;
• sanzione disciplinare grave;
• accesso alla commissione di garanzia;
• segnalazione alle forze dell'ordine.

La Legge 71/2017, nell'articolo 2, cui si rimanda, indica tempi e modalità per richiedere la rimozione di contenuti ritenuti dannosi per i minori.
La Legge 71/2017, agli articoli 5 e 7, cui si rimanda, riporta due sanzioni nei confronti dei trasgressori della legge stessa, minorenni e di età superiore ai quattordici anni (rispettivamente sanzioni disciplinari in ambito scolastico con percorsi di recupero, ammonimento presso il Questore).
La scuola potrà, altresì, segnalare episodi di cyberbullismo nonché la eventuale presenza di materiale pedopornografico in rete al servizio Helpline di Telefono Azzurro1.96.96 e/o a Save the Children che mette a disposizione "Stop-It", la Hotline attiva dal 2001 all'indirizzo www.stop-it.it, affinché trasmettano dette segnalazioni al Centro Nazionale per il Contrasto alla Pedopornografia su Internet, istituito presso la Polizia Postale e delle Comunicazioni, per consentire le attività di investigazione necessarie.
Le azioni individuate hanno la finalità di sostenere le vittime, le famiglie e tutti coloro che sono stati spettatori attivi o passivi di quanto avvenuto, e di realizzare interventi educativi nei confronti di coloro che hanno messo in atto comportamenti lesivi del rispetto degli altri.
I docenti del team predisporranno specifiche rilevazioni ed azioni preventive sulla base dei protocolli suggeriti dalla piattaforma prevista nell'ambito del progetto Elisa (formazione E- Learning degli Insegnanti sulle Strategie Antibullismo), nata grazie alla collaborazione tra il MI- Direzione generale per lo studente e il Dipartimento di Formazione, Lingue, Intercultura, Letterature e Psicologia dell'Università di Firenze.

MONITORAGGIO DELL'IMPLEMENTAZIONE ALLA POLICYE SUO AGGIORNAMENTO

La E-Safety Policy si inserisce all'interno di altre politiche scolastiche , quali la politica antibullismo e la politica del benessere degli alunni a scuola

- la scuola ha un docente della sicurezza online che si prenderà cura della revisione e/o aggiornamento della della Policy sotto la super visione del DS
- la E-Safety Policy sarà riesaminata annualmente o quando si verificano cambiamenti significativi per quanto riguarda le tecnologie in uso all'interno della scuola e le eventuali modifiche saranno discusse con i membri del personale docente

Nell'ambito della revisione della Policy, tutte le informazioni e le revisioni saranno memorizzate per eventuali controlli, sulla base del seguente documento

NOME	E-SAFETY POLICY ISS F. VIGANO'
VERSIONE	
AUTORE	Nome del docente responsabile della sicurezza online (E-Safety Policy)
APPROVATO DAL DIRIGENTE	
APPROVATO DAL COLLEGIO DOCENTI	
PROSSIMA DATA DI REVISIONE	
MODIFICA	Esplicitare versione, data, descrizione, nome docente responsabile…

INTEGRAZIONE DELLA POLICY CON REGOLAMENTI ESISTENTI
REGOLAMENTO DI ISTITUTO: l'E- Policy verrà allegata al regolamento di Istituto e ne sarà parte integrante.

2. FORMAZIONE E CURRICOLO

CURRICOLO DELLE COMPETENZE DIGITALI PER GLI STUDENTI
Al termine del corso di studi gli alunni conseguiranno competenze digitalipreviste dai piani di lavoro dei docenti di informatica.

FORMAZIONE DOCENTI
Al fine di favorire il continuo aggiornamento sui temi delle tecnologie digitali, sia in termini di utilizzo ed integrazione delle TSI (Tecnologie della Società dell'informazione) nella didattica, sia di utilizzo consapevole e sicuro di Internet e delle tecnologie digitali, verranno promosse iniziative volte al confronto ed allo scambio di idee e pratiche innovative:

- attività formative interne (seminari, workshop, attività laboratoriali), avvalendosi di risorse interne e/o esterne
- diffusione di informazioni circa opportunità formative esterne in presenza e/o a distanza.

SENSIBILIZZAZIONE DELLE FAMIGLIE
In considerazione dell'importanza di favorire la sinergia degli interventi educativi di Scuola e famiglia per il successo scolastico ed educativo di ogni studente, il presente documento è allegato al Patto Educativo di Corresponsabilità stipulato con le famiglie degli alunni quale l'impegno reciproco di scuola e famiglia alla corresponsabilità formativa, nella quale rientrano a pieno titolo i temi legati alla eSafety.

3. INFRASTRUTTURA E STRUMENTAZIONE TIC (O ICT)

ACCESSO A INTERNET: FILTRI ANTIVIRUS E SULLA NAVIGAZIONE
- L'accesso a internet è possibile in tutte le aule dell'Istituto, nei laboratori d'informatica e negli uffici.
- Il responsabile del laboratorio di informatica imposta i computer (filtri antivirus) per l'utilizzo ma è responsabilità di ogni docente segnalarne eventuali malfunzionamenti e disservizi. I docenti hanno piena autonomia nel collegamento ai siti web nelle postazioni a loro riservate.
- Agli alunni che accedono a internet durante l'attività didattica sono consentiti la navigazione guidata e la stesura di documenti, purché sotto il controllo dell'insegnante e solo nel caso in cui tale attività faccia parte di un progetto di lavoro precedentemente autorizzato.

GESTIONE ACCESSI: PASSWORD, BACKUP, ecc...
- Ai docenti è consentito accedere ad Internet tramite i dispositivi scolastici (postazioni fisse, pc portatili, tablet, regolati da password create con criteri standard) oppure da un proprio dispositivo, utilizzando la rete wi-fi dell'Istituto.
- La connessione wi-fi ad Internet è regolata da un meccanismo di autenticazione autorizzazione attraverso il rilascio di una password da parte dell'ufficio tecnico.
- Al termine delle ore di lezione il docente deve verificare lo spegnimento dei dispositivi messi a disposizione dalla scuola.
- Gli studenti possono accedere alla rete Internet tramite i dispositivi scolastici, solo dietro autorizzazione e sotto il controllo di un docente.

E-MAIL
L'account di posta elettronica è solo quello istituzionale.

BLOG E SITO WEB DELLA SCUOLA
- Il sito prevede un'area in cui sono reperibili le informazioni sulla vita scolastica, iniziative e scadenze ministeriali, avvisi di carattere generale. Nel sito è presente anche un'area riservata relativa al Registro Elettronico accessibile solo previa autenticazione sia per i docenti sia per le famiglie.
- Il personale che è in possesso delle credenziali per la gestione dei contenuti del portale si assume la responsabilità editoriale di garantire che il contenuto inserito sia accurato e appropriato.

- Il Dirigente Scolastico e il personale incaricato di gestire le pagine del Sito hanno la responsabilità di garantire che il contenuto pubblico sia accurato e appropriato.
- L'Istituto risponde solo dei contenuti pubblicati sul sito istituzionale.

SOCIAL NETWORK

Sono accettati i social ufficiali dell'Istituto quali "Meet" su Google Classroom e "Teams" su Office 365 o "Webex" di Cisco System.

PROTEZIONE DATI PERSONALI

- Il trattamento dei dati personali riguarda unicamente le finalità istituzionali della scuola, i dati saranno trattati secondo le modalità previste dal DPGR Regolamento Europeo 679/2016.
- Tutto il personale è tenuto a conoscere la normativa riguardante il trattamento dei dati personali ai fini della protezione e sicurezza degli stessi.
- In caso di attività di ampliamento dell'Offerta Formativa, organizzate in collaborazione con Enti esterni, viene richiesto preventivamente ai genitori il consenso alle riprese audio/ video e al loro eventuale utilizzo per scopi didattici, informativi e divulgativi.
- L'accesso ai dati riportati nel registro elettronico (ritardi, assenze, note, valutazioni, ecc.) è riservato ai genitori a cui sono consegnate credenziali di accesso strettamente personali.

A integrazione dell'informativa ex art 13 del Reg. UE 2016/679, si ribadisce che i dati personali sono trattati in modo lecito, corretto e trasparente, che sono raccolti per finalità determinate, esplicite e legittime, che sono trattati in modo non incompatibile con tali finalità, evitando qualsiasi forma di profilazione, nonché di diffusione e comunicazione dei dati personali raccolti a tal fine, che essi sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per cui sono trattati, e trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.
Nell'ottica di favorire lo sviluppo delle competenze digitali, la creazione e la condivisione sia di risorse sia della documentazione didattica, l'Istituto "Francesco Viganò" ha attivato una serie di servizi e piattaforme digitali gratuite.
L'obiettivo di questa iniziativa è ottimizzare, attraverso le tecnologie di rete, sia l'attività didattica sia la circolazione delle informazioni interne, come comunicazioni, documentazione e didattica tramite uso di applicazioni specifiche.
Infatti, come prevede la nota del Ministero dell'Istruzione n. 279 del 08.03.2020, il protrarsi della situazione di emergenza che stiamo vivendo comporta la necessità di attivare la didattica a distanza che non deve limitarsi alla mera trasmissione di compiti ed esercitazioni.
Le procedure con le quali attivare tali strumenti – utilizzo della piattaforma Google Suite (Classroom, Meet, Hangouts), dell'applicazione Teams di Office365 o di Webex di Cisco System – saranno tempestivamente comunicate sul registro elettronico, che si prega di mantenere monitorato.
Il presente documento ha la finalità di stabilire delle regole di comportamento, atte a strutturare un lavoro comune ben organizzato tra Studenti e Docenti.
Inoltre, al fine di procedere all'attivazione degli strumenti digitali, chiediamo la collaborazione di tutti che, dopo avere letto attentamente le regole sottoindicate, dovranno rispettarle, tenendo presente che la durata dell'account/link per l'uso di tali

strumenti è conforme al periodo di chiusura delle attività didattiche tradizionali previsto dal DPCM 08/03/2020 art.2 lettera m e sgg.

UTILIZZO DELLE PIATTAFORME DI DIDATTICA A DISTANZA
Modalità di utilizzo
Le procedure per accedere a tutte le risorse digitali saranno comunicate tramite registro elettronico.

Obblighi dello Studente.
Lo Studente si impegna:
• a non divulgare ad altre persone le procedure per l'utilizzo degli strumenti digitali in uso;
• a comunicare immediatamente malfunzionamenti degli strumenti digitali;
• a non consentire ad altri, a nessun titolo, l'utilizzo delle piattaforme o delle applicazioni a cui accede;
• a non diffondere eventuali informazioni riservate di cui venisse a conoscenza, relative all'attività delle altre persone che utilizzano il servizio;
• ad osservare il presente regolamento;
• ad utilizzare i servizi offerti solo ad uso esclusivo per le attività didattiche della scuola;
• lo Studente e la sua famiglia si assumono la piena responsabilità di tutti i dati inoltrati dallo Studente stesso, creati e gestiti attraverso le piattaforme e le applicazioni.

Limiti di responsabilità.
L'Istituto non risponde di eventuali disservizi o malfunzionamenti delle piattaforme utilizzate.
Tutti i documenti prodotti dai docenti dell'Istituto (ad es. slide, testi, video lezioni predisposte su You Tube o altre piattaforme, lezioni in diretta, ecc..) saranno inviati o effettuati all'interno o tramite le piattaforme predisposte dall'Istituto.
Pertanto, l'uso improprio del materiale suddetto e/o in violazione del presente Regolamento, del Regolamento d'Istituto e/o della normativa vigente in materia di tutela della privacy e/o la pubblicazione dei materiali suddetti su altri siti o la loro diffusione tramite qualsiasi canale diverso da quelli indicati in precedenza, farà insorgere in capo all'autore di tali condotte e al tutore legale responsabilità civili e/o penali a seconda della tipologia di comportamento posto in essere nel caso specifico. Conseguentemente, nessuna responsabilità sarà attribuibile all'Istituto stesso.

Netiquette per lo Studente.
Di seguito sono riportate le regole di comportamento che ogni studente deve seguire affinché i servizi digitali possano funzionare nel migliore dei modi, considerando che le norme di cortesia e buona educazione, che regolano i rapporti umani, restano validi anche in questo contesto.
Poiché i servizi digitali sono uno dei mezzi di comunicazione tra i Docenti e lo Studente, sarà dovere di ciascuno accedere al registro elettronico possibilmente con frequenza quotidiana, impegnandosi a rispettare la seguente netiquette:
• inviare messaggi brevi che descrivano in modo chiaro l'oggetto della comunicazione; indicando sempre chiaramente l'oggetto del messaggio stesso, in modo tale che il destinatario possa immediatamente individuare l'argomento della mail ricevuta;

• non inviare mai lettere o comunicazioni provenienti da catene (ad esempio catene di S. Antonio o altri sistemi a carattere "piramidale") che causerebbero un inutile aumento del traffico in rete;
• non utilizzare le piattaforme o le applicazioni in modo da danneggiare, molestare o insultare altre persone;
• non creare e non trasmettere immagini, dati o materiali non rispettosi della dignità e del decoro dell'Istituto e delle persone;
• non creare e non trasmettere materiale offensivo per altre persone o enti;
• non creare e non trasmettere materiale commerciale o pubblicitario;
• in caso di condivisione di documenti, non interferire, danneggiare o distruggere il lavoro dei Docenti o degli altri Studenti;
• non curiosare nei file e non violare la riservatezza degli altri Studenti;
• utilizzare il PC, le piattaforme e le applicazioni in modo da mostrare considerazione e rispetto per gli altri Studenti e i Docenti;
• durante una videoconferenza partecipare tenendo la webcam accesa, su richiesta del Docente e accendere il microfono solo per poter interagire durante la lezione ;
• durante la lezione in videoconferenza, è assolutamente vietato registrare video del docente senza il suo permesso. Violare il diritto d'autore del tuo insegnante e la sua privacy comporta le sanzioni penali e pecuniarie previste all'art. 83 del Regolamento della Comunità Europea 2016/679 e dal Codice della privacy (D.Lgs 196/2003) Parte III così come modificato e integrato dal D.Lgs 101/2018.

4. DISPOSITIVI PERSONALI

STUDENTI
Gli alunni possono portare il dispositivo (smartphone) a scuola, che deve essere tenuto spento e nello zaino durante le lezioni, a meno che, per esigenze didattiche, il docente non ne consenta l'uso.
Si recepisce in questo documento quanto previsto dalla Direttiva Ministeriale n. 30 del 15marzo 2007: "le famiglie si assumono l'impegno di rispondere direttamente dell'operato dei propri figli nel caso in cui, ad esempio, gli stessi arrechino danni ad altre persone".

DOCENTI
Non è consentito l'uso del dispositivo (smartphone) durante le ore di lezione tranne per motivi lavorativi. È consentito l'uso di altri dispositivi elettronici personali solo a scopo didattico ed integrativo di quelli scolastici disponibili. Per il restante orario di servizio è consentito l'uso del dispositivo (smartphone) solo per importanti comunicazioni personali urgenti.

PERSONALE DELLA SCUOLA
Il personale scolastico è autorizzato ad usare il proprio dispositivo se non sta svolgendo un ruolo didattico, solo se l'utilizzo non intralci il normale svolgimento delle attività scolastiche, né distragga dal corretto svolgimento delle proprie mansioni.

5. PREVENZIONE, RILEVAZIONE, GESTIONE CASI

Per i ragazzi nativi digitali le interconnessioni tra vita e tecnologia sono la normalità. Essi, pur essendo spesso tecnicamente competenti, tendono a non cogliere le implicazioni dei loro comportamenti e tale fenomeno è tanto maggiore quanto è più forte il coinvolgimento emotivo nell'utilizzo dei nuovi media. Ciò fa sì che alcuni rischi che fanno parte del mondo digitale possano non essere percepiti come tali ed è dunque compito degli adulti, famiglie ed insegnanti, affrontarli con l'obiettivo di prevenirli.

Tra i principali rischi, sia di carattere comportamentale che di matrice tecnica, ricordiamo:
• possibile esposizione a contenuti violenti e non adatti alla loro età;
• videogiochi diseducativi;
• pubblicità ingannevoli;
• accesso ad informazioni scorrette;
• virus informatici in grado di infettare computer e cellulari;
•adescamento online
• rischio di molestie o maltrattamenti da coetanei (bullismo e cyberbullismo);
• scambio di materiale a sfondo sessuale (sexting);
• uso eccessivo di Internet/cellulare (dipendenza).

PREVENZIONE
Come azione di prevenzione universale la scuola ha attivato diversi progetti/attività

- Progetto Cyberbullismo
- Progetto Educazione alla salute
- Progetto Armonia
- Progetto Legalità
- Progetto Violenza di genere
- Attività CIC

RILEVAZIONE
Laddove il docente/personale della scuola/ familiare/alunno colga possibili situazioni di disagio connesse ad uno o più di uno tra i rischi elencati nel paragrafo "Prevenzione", potrà chiedere il supporto al Team per il bullismo e cyberbullismo, compilando la "scheda di segnalazione" (disponibile sul sito web istituzionale).

GESTIONE DEI CASI
A seguito della segnalazione, il docente Referente insieme al suo team avrà cura di pianificare adeguati interventi educativi e, ove necessario, di coinvolgere le famiglie per l'attivazione di un percorso comune e condiviso di sostegno al disagio.
Le azioni poste in essere dalla Scuola saranno dirette non solo a supportare le vittime, le famiglie e tutti coloro che sono stati spettatori attivi o passivi di quanto avvenuto, ma anche a realizzare interventi educativi rispetto a quanti abbiano messo in atto comportamenti lesivi, ove si tratti di soggetti interni all'Istituto.
Nel casi di maggiore gravità si valuterà anche il coinvolgimento di attori esterni quali le forze dell'ordine e i servizi sociali

6. ALLEGATI:

a. Prima segnalazione dei casi di (presunto) bullismo o vittimizzazione.
b. Valutazione approfondita
c. Referenti del team contro il cyberbullismo
d. Referenti sul territorio contro il cyberbullismo
e. Scheda di Monitoraggio
f. Modello di segnalazione al Garante della privacy