



# Istituto di Istruzione Secondaria Superiore **UGO FOSCOLO**

**LICEI DI CANICATTI'**

Scientifico - Classico - Linguistico

Via Pirandello, 6 - 92024 Canicatti (AG)

Cod. Ministeriale AGIS00100X - Cod. Fiscale 82002070843

Sede centrale via Pirandello Tel.0922 851006 – Sede via Pasolini Tel. 0922 855515

web:<http://www.liceocanicatti.edu.it> – [agis00100x@istruzione.it](mailto:agis00100x@istruzione.it) - [agis00100x@pec.istruzione.it](mailto:agis00100x@pec.istruzione.it)

# eSafety

# Policy

Documento approvato dal collegio dei docenti con delibera n. 3 del 20.05.2019

Documento approvato dal Consiglio d'Istituto con delibera n. .... del .....

## **1.Elementi generali dell'E-safety Policy**

### **- Scopo della e-safety policy**

Scopo del presente documento è quello di informare l'utenza per un uso corretto e responsabile delle apparecchiature informatiche collegate alla rete in dotazione alla Scuola, nel rispetto della normativa vigente.

In particolare, l'intento della scuola è quello di promuovere l'uso consapevole e critico da parte degli alunni delle tecnologie digitali e di internet, di far acquisire loro procedure e competenze "tecniche" ma anche corrette norme comportamentali, di prevenire ovvero rilevare e fronteggiare le problematiche che derivano da un utilizzo non responsabile, pericoloso o dannoso, delle tecnologie digitali. Gli utenti, siano essi maggiorenni o minori, devono essere pienamente consapevoli dei rischi a cui si espongono quando navigano in rete. Di fatto esiste la possibilità che durante il lavoro online si possa entrare accidentalmente in contatto con materiale inadeguato e/o illegale, pertanto la Scuola promuove l'adozione di strategie che limitino l'accesso a siti e/o applicazioni illeciti. In questo contesto, gli insegnanti hanno la responsabilità di guidare gli studenti nelle attività online a scuola e di indicare regole di condotta chiare per un uso critico e consapevole di Internet anche a casa, per prevenire il verificarsi di situazioni potenzialmente pericolose.

### **- Ruoli e Responsabilità (che cosa ci si aspetta da tutti gli attori della Comunità Scolastica)**

#### 1) Dirigente scolastico

Il ruolo del Dirigente scolastico nel promuovere l'uso consentito delle tecnologie e di internet include i seguenti compiti:

- garantire la sicurezza (tra cui la sicurezza on-line) dei membri della comunità scolastica;
- garantire che tutti gli insegnanti ricevano una formazione adeguata per svolgere efficacemente l'insegnamento volto a promuovere una cultura dell'inclusione, del rispetto dell'altro/a e delle differenze, un utilizzo positivo e responsabile delle Tecnologie dell'Informazione e della comunicazione (TIC);
- garantire l'esistenza di un sistema in grado di consentire il monitoraggio e il controllo interno della sicurezza on-line;
- comprendere e seguire le procedure previste dalle norme in caso di reclami o attribuzione di responsabilità al personale scolastico in relazione a incidenti occorsi agli alunni nell'utilizzo delle TIC a scuola.

## 2) Animatore digitale

Il ruolo dell'Animatore digitale include i seguenti compiti:

- stimolare la formazione interna all'istituzione negli ambiti di sviluppo della “scuola digitale” e fornire consulenza e informazioni al personale in relazione ai rischi on-line e alle misure di prevenzione e gestione degli stessi;
- monitorare e rilevare le problematiche emergenti relative all'utilizzo sicuro delle tecnologie digitali e di internet a scuola, nonché proporre la revisione delle politiche dell'istituzione con l'individuazione di soluzioni metodologiche e tecnologiche innovative e sostenibili da diffondere nella scuola;
- assicurare che gli utenti possano accedere alla rete della scuola solo tramite password applicate e regolarmente cambiate e curare la manutenzione e lo sviluppo del sito web della scuola per scopi istituzionali e consentiti (istruzione e formazione);
- coinvolgere la comunità scolastica (alunni, genitori e altri attori del territorio) nella partecipazione ad attività e progetti attinenti la “scuola digitale”.

## 3) Referente del Bullismo e Cyberbullismo

- Promuove la conoscenza e la consapevolezza del bullismo e del cyber-bullismo attraverso progetti d'istituto che coinvolgano genitori, studenti e tutto il personale;
- Promuovere l'educazione all'uso consapevole della rete internet e l'educazione ai diritti e ai doveri legati all'utilizzo delle tecnologie informatiche
- Coordina le attività di prevenzione ed informazione sulle sanzioni previste e sulle responsabilità di natura civile e penale, anche con eventuale affiancamento di genitori e studenti;
- Si rivolge a partner esterni alla scuola, quali servizi sociali e sanitari, aziende del privato sociale, forze di polizia, per realizzare azioni di prevenzione;
- Cura rapporti di rete fra scuole per eventuali convegni/seminari/corsi.

## 4) Consiglio di classe

- Pianifica attività didattiche e/o integrative finalizzate al coinvolgimento attivo e collaborativo degli studenti e all'approfondimento di tematiche che favoriscano la riflessione e la presa di coscienza della necessità dei valori di convivenza civile;
- Favorisce un clima collaborativo all'interno della classe e nelle relazioni con le famiglie.

## 5) DSGA e personale ATA

Il ruolo del direttore dei servizi generali e amministrativi include i seguenti compiti:

- assicurare, nei limiti delle risorse finanziarie disponibili, l'intervento di tecnici per garantire che l'infrastruttura tecnica della scuola sia funzionante, sicura e non aperta a uso improprio o a dannosi attacchi esterni;
- garantire il funzionamento dei diversi canali di comunicazione della scuola (sportello, circolari, sito web, ecc.) all'interno della scuola e fra la scuola e le famiglie degli alunni per la notifica di documenti e informazioni del Dirigente scolastico e dell'Animatore digitale nell'ambito dell'utilizzo delle tecnologie digitali e di internet.

Il personale ATA deve conoscere l'E-Safety Policy per contribuire alla sorveglianza:

- i collaboratori scolastici vigilano sui comportamenti tenuti dagli alunni e riferiscono tempestivamente al Dirigente, al Referente per Cyberbullismo e all'Animatore Digitale.

## 6) Docenti

Il ruolo del personale docente e di ogni figura educativa che lo affianca include i seguenti compiti:

- informarsi/aggiornarsi sulle problematiche attinenti alla sicurezza nell'utilizzo delle tecnologie digitali e di internet e sulla politica di sicurezza adottata dalla scuola, rispettandone il regolamento;
- garantire che le modalità di utilizzo corretto e sicuro delle TIC e di internet siano integrate nel curriculum di studio e nelle attività didattiche ed educative delle classi;
- garantire che gli alunni capiscano e seguano le regole per prevenire e contrastare l'utilizzo scorretto e pericoloso delle TIC e di internet;
- assicurare che gli alunni abbiano una buona comprensione delle opportunità di ricerca offerte dalle tecnologie digitali e dalla rete ma anche della necessità di evitare il plagio e di rispettare la normativa sul diritto d'autore;
- 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;
- assicurare la riservatezza dei dati personali trattati ai sensi della normativa vigente;
- controllare l'uso delle tecnologie digitali, dispositivi mobili, macchine fotografiche, ecc. da parte degli alunni durante le lezioni e ogni altra attività

scolastica (ove consentito);

- nelle lezioni in cui è programmato l'utilizzo di Internet, guidare gli alunni a siti controllati e verificati come adatti per il loro uso e controllare che nelle ricerche su Internet siano trovati e trattati solo materiali idonei;
- comunicare ai genitori difficoltà, bisogni o disagi espressi dagli alunni (ovvero valutazioni sulla condotta non adeguata degli stessi) rilevati a scuola e connessi all'utilizzo delle TIC, al fine di approfondire e concordare coerenti linee di intervento di carattere educativo;
- segnalare qualsiasi problema o proposta di carattere tecnico-organizzativo ovvero esigenza di carattere informativo all'Animatore digitale ai fini della ricerca di soluzioni metodologiche e tecnologiche innovative da diffondere nella scuola e di un aggiornamento della politica adottata in materia di prevenzione e gestione dei rischi nell'uso delle TIC;
- segnalare al Dirigente scolastico e ai genitori qualsiasi abuso rilevato a scuola nei confronti degli alunni in relazione all'utilizzo delle tecnologie digitali o di internet, per l'adozione delle procedure previste dalle norme.

## 7) Alunni

Il ruolo degli alunni include i seguenti compiti:

- essere responsabili, in relazione al proprio grado di maturità e di apprendimento, per l'utilizzo dei 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 per non correre rischi;
- adottare condotte rispettose degli altri anche quando si comunica in rete;
- esprimere domande o difficoltà o bisogno di aiuto nell'utilizzo delle tecnologie didattiche o di internet ai docenti e ai genitori.
- Conoscere e rispettare l'E-Safety Policy e segnalare al docente di classe eventuali usi impropri della rete e dei dispositivi.

## 8) Genitori

Il ruolo dei genitori degli alunni include i seguenti compiti:

- Sostenere la linea di condotta della scuola adottata nei confronti dell'utilizzo delle tecnologie dell'Informazione e delle Comunicazioni nella didattica;
- Seguire gli alunni nello studio a casa adottando i suggerimenti e le condizioni d'uso delle TIC indicate dai docenti, in particolare controllare l'utilizzo del pc e di internet;
- Concordare con i docenti linee di intervento coerenti e di carattere educativo in relazione ai problemi rilevati per un uso non responsabile o pericoloso delle tecnologie digitali o di internet;
- Fissare delle regole per l'utilizzo del computer e tenere sotto controllo l'uso che i figli fanno di internet e del telefonino in generale.

**- Condivisione e comunicazione della Policy all'intera comunità scolastica.**

1) Condividere e comunicare la politica di e-safety agli alunni

- Tutti gli alunni saranno informati che la rete, l'uso di Internet e di ogni dispositivo digitale saranno controllati dagli insegnanti e utilizzati solo con la loro autorizzazione.
- L'istruzione degli alunni riguardo all'uso responsabile e sicuro di internet precederà l'accesso alla rete;
- L'elenco delle regole per la sicurezza on-line sarà pubblicato in tutte le aule o laboratori con accesso a internet;
- Sarà data particolare attenzione nell'educazione sulla sicurezza agli aspetti per i quali gli alunni risultano più esposti o rispetto ai quali risultano più vulnerabili.

2) Condividere e comunicare la politica di e-safety al personale

- La linea di condotta della scuola in materia di sicurezza nell'utilizzo delle tecnologie digitali e di internet sarà discussa negli organi collegiali (consigli di classe, collegio dei docenti) e comunicata formalmente a tutto il personale con il presente documento e altro materiale informativo anche sul sito web;
- Per proteggere tutto il personale e gli alunni, la scuola metterà in atto una linea di condotta di utilizzo accettabile, controllato e limitato alle esigenze didattiche essenziali;
- Il personale docente sarà reso consapevole del fatto che il traffico in internet può essere monitorato e si potrà risalire al singolo utente registrato;
- Il sistema di filtraggio adottato e il monitoraggio sull'utilizzo delle TIC sarà

supervisionato dall'Animatore digitale, che segnalerà al DSGA eventuali problemi che dovessero richiedere acquisti o interventi di tecnici;

- L'Animatore digitale metterà in evidenza on-line utili strumenti che il personale potrà usare con gli alunni in classe.
- Tutto il personale è consapevole che una condotta non in linea con il codice di comportamento dei pubblici dipendenti e i propri doveri professionali è sanzionabile.

### 3) Condividere e comunicare la politica di e-safety ai genitori

- L'attenzione dei genitori sulla sicurezza nell'uso delle tecnologie digitali e di internet sarà attirata nelle news o in altre aree del sito web della scuola;
- Sarà incoraggiato un approccio di collaborazione nel perseguimento della sicurezza nell'uso delle TIC e di internet in occasione degli incontri scuola-famiglia, assembleari, collegiali e individuali;
- L'Animatore digitale fornirà ai genitori suggerimenti e indicazioni per l'uso sicuro delle tecnologie digitali e di internet anche a casa;

## **- Gestione delle infrazioni alla Policy.**

### 1) Disciplina degli alunni

Le potenziali infrazioni in cui è possibile che gli alunni incorrano a scuola nell'utilizzo delle tecnologie digitali di internet di cui si dispone per la didattica, in relazione alla fascia di età considerate, sono prevedibilmente le seguenti:

- un uso della rete per giudicare, infastidire o impedire a qualcuno di esprimersi o partecipare;
- l'invio incauto o senza permesso di foto o di video di altri dati personali come l'indirizzo di casa o il telefono;
- la condivisione di immagini intime o troppo spinte;
- la comunicazione incauta e senza permesso con sconosciuti;
- il collegamento a siti web non indicati dai docenti;
- la registrazione di video non autorizzati durante lo svolgimento delle lezioni;
- uso di linguaggio aggressivo e offensivo esercitato tramite social network.

Gli interventi correttivi previsti per gli alunni sono rapportati all'età e al livello di sviluppo dell'alunno.

Sono previsti pertanto provvedimenti "disciplinari" proporzionati all'età e alla gravità del

comportamento, quali:

- il richiamo verbale o ammonizione;
- provvedimenti del consiglio di classe con particolari conseguenze (riduzione o sospensione dell'attività gratificante quali esclusione da visite e viaggi di istruzione e/o atti riparatori);
- la convocazione dei genitori da parte degli insegnanti;
- la convocazione dei genitori da parte del Dirigente scolastico;
- la sospensione delle lezioni con (o senza) obbligo di frequenza;
- l'ammonimento del questore.

Contestualmente sono previsti interventi di carattere educativo di rinforzo dei comportamenti corretti e riparativi dei disagi causati, di ridefinizione delle regole sociali di convivenza attraverso la partecipazione consapevole e attiva degli alunni della classe, di prevenzione e gestione positiva dei conflitti, di moderazione dell'eccessiva competitività, di promozione di rapporti amicali e di reti di solidarietà, di promozione della conoscenza e della gestione delle emozioni.

Si precisa che per i minori autori di atti di cyberbullismo, fra i 14 e i 18 anni, se non c'è querela o denuncia per i reati di cui agli articoli 594, 595 e 612 del codice penale, scatta l'ammonimento: il questore convoca il minore insieme ad almeno un genitore.

## 2) Disciplina del personale scolastico

Le potenziali infrazioni in cui è possibile che il personale scolastico e in particolare i docenti incorrano nell'utilizzo delle tecnologie digitali e di internet sono diverse e alcune possono determinare, favorire o avere conseguenze di maggiore o minore rilievo sull'uso corretto e responsabile delle TIC da parte degli alunni:

- un utilizzo delle tecnologie e dei servizi della scuola, d'uso comune con gli alunni, non connesso alle attività di insegnamento o al profilo professionale, anche tramite installazione di software o il salvataggio di materiali non idonei;
- un utilizzo delle comunicazioni elettroniche con i genitori e gli alunni non compatibile con il ruolo professionale;
- un trattamento dei dati personali, comuni e sensibili degli alunni, non conforme ai principi della privacy o che non garantisca un'adeguata protezione degli stessi;
- una diffusione delle password assegnate e una custodia non adeguata degli strumenti e degli accessi di cui possono approfittare terzi;
- una carente istruzione preventiva degli alunni sull'utilizzazione corretta e responsabile delle tecnologie digitali e di internet;
- una vigilanza elusa dagli alunni che può favorire un utilizzo non autorizzato delle TIC e possibili



incidenti;

- insufficienti interventi nelle situazioni critiche di contrasto a terzi, correttivi o di sostegno agli alunni, di segnalazione ai genitori, al Dirigente scolastico, all'Animatore digitale.

Il Dirigente scolastico può controllare l'utilizzo delle TIC per verificarne la conformità alle regole di sicurezza, compreso l'accesso a internet, la posta elettronica inviata/pervenuta a scuola, procedere alla cancellazione di materiali inadeguati o non autorizzati dal sistema informatico della scuola, conservandone una copia per eventuali successive investigazioni.

Tutto il personale è tenuto a collaborare con il Dirigente scolastico e a fornire ogni informazione utile per le valutazioni del caso e per l'avvio di procedimenti che possono avere carattere organizzativo gestionale, disciplinare, amministrativo, penale, a seconda del tipo o della gravità delle infrazioni commesse. Le procedure sono quelle previste dalla legge e dai contratti di lavoro.

### 3) Disciplina dei genitori

In considerazione dell'età degli alunni e della loro dipendenza dagli adulti, anche alcune condizioni e condotte dei genitori possono favorire o meno l'uso corretto e responsabile delle TIC da parte degli alunni a scuola, dove possono portare materiali e strumenti o comunicare problematiche sorte al di fuori del contesto scolastico.

Le situazioni familiari meno favorevoli sono:

- la convinzione che se il proprio figlio rimane a casa ad usare il computer è al sicuro e utilizza con responsabilità le TIC;
- una posizione del computer in una stanza o in un posto non visibile a tutti quando è utilizzato dal proprio figlio;
- una piena autonomia concessa al proprio figlio nella navigazione sul web e nell'utilizzo del cellulare o dello smartphone;
- un utilizzo del pc in comune con gli adulti che possono conservare in memoria materiali non idonei;
- un utilizzo del cellulare o dello smartphone in comune con gli adulti che possono conservare in memoria indirizzi o contenuti non idonei.

I genitori degli alunni possono essere convocati a scuola, o dal questore, per concordare misure educative diverse oppure essere sanzionabili a norma di legge in base alla gravità dei comportamenti dei loro figli, se dovessero risultare pericolosi per sé e/o dannosi per gli altri.

#### **- Monitoraggio dell'implementazione della Policy e suo aggiornamento.**

Il monitoraggio dell'implementazione della policy e del suo eventuale aggiornamento sarà

svolto ogni anno. Tale monitoraggio sarà curato dal Dirigente scolastico con la collaborazione dell'Animatore digitale, del Referente sul Cyberbullismo e dai docenti delle classi, tramite questionari e conversazioni. Sarà finalizzato a rilevare la situazione iniziale delle classi e gli esiti a fine anno, in relazione all'uso sicuro e responsabile delle tecnologie digitali e di internet. Il monitoraggio sarà rivolto anche agli insegnanti, al fine di valutare l'impatto della policy e la necessità di eventuali miglioramenti. L'aggiornamento della policy sarà curato dal Dirigente scolastico, dall'Animatore digitale, dagli Organi Collegiali, a seconda degli aspetti considerati.

## 2. Formazione e Curricolo

### **- Curricolo sulle competenze digitali per gli studenti**

*“La competenza digitale consiste nel saper utilizzare con dimestichezza e spirito critico le tecnologie della società dell’informazione (TSI) per il lavoro, il tempo libero e la comunicazione. Essa è supportata da abilità di base nelle TIC: l’uso del computer per reperire, valutare, conservare, produrre, presentare e scambiare informazioni nonché per comunicare e partecipare a reti collaborative tramite Internet”.*

Le competenze digitali rientrano tra le competenze chiave di cittadinanza (Raccomandazione del Parlamento Europeo e del Consiglio del 22 maggio 2018) e, come tali, vengono promosse trasversalmente da tutti i docenti.

Le competenze digitali vengono certificate sulla base dei seguenti descrittori:

lo studente:

- sa utilizzare responsabilmente gli strumenti e i servizi a disposizione
- sa proteggere la propria immagine e i propri dati personali
- mostra senso critico dinanzi all'informazione e al suo trattamento
- sa utilizzare e produrre dati
- rispetta il copyright

### **- Formazione dei docenti sull’utilizzo e l’integrazione delle TIC nella didattica**

Il corpo docente ha partecipato a corsi di formazione anche nell’ambito di piani nazionali, oltre che ad iniziative organizzate dall’istituzione o dalle scuole associate in rete e possiede generalmente una buona base di competenze e nel caso delle figure di sistema, anche di carattere specialistico. E’ inoltre disponibile ad aggiornarsi per mantenere al passo la propria formazione, in rapporto al rinnovo della dotazione multimediale.

Il percorso complesso della formazione specifica dei docenti sull’utilizzo delle TIC nella didattica, non esauribile nell’arco di un anno scolastico, può pertanto prevedere momenti di autoaggiornamento, momenti di formazione personale o collettiva anche all’interno dell’istituto, con la condivisione delle conoscenze dei singoli e il supporto dell’Animatore digitale, la partecipazione alle iniziative promosse dall’Amministrazione centrale e dalle scuole polo; può comprendere altresì la fruizione dei materiali messi a disposizione dall’Animatore stesso sulle bacheche virtuali appositamente create, corsi di aggiornamento online.

### **- Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali**

Anche il percorso della formazione specifica dei docenti sull'utilizzo consapevole e sicuro di Internet, può prevedere momenti di autoaggiornamento, momenti di formazione personale o collettiva di carattere permanente, legata all'evoluzione rapida delle tecnologie e delle modalità di comunicazione a cui accedono sempre di più ed autonomamente anche i ragazzi.

Sul sito della scuola è possibile trovare materiali informativi sulla sicurezza in internet per l'approfondimento personale, per le attività con gli studenti e gli incontri con i genitori, costituiti da guide in pdf, video, manuali a fumetti, link a siti specializzati e contributi della Polizia di Stato, dell'Arma dei Carabinieri, di Telefono Azzurro, dal sito "Generazioni connesse".

### **- Sensibilizzazione delle famiglie**

L'Istituto attiverà iniziative per sensibilizzare le famiglie all'uso consapevole delle TIC e della rete, promuovendo la conoscenza delle numerose situazioni di rischio online. A tal fine sono previsti incontri fra docenti e genitori per la diffusione del materiale informativo sulle tematiche trattate, messo a disposizione dai siti specializzati e dalle forze dell'ordine.

Saranno favoriti momenti di confronto e discussione anche sulle dinamiche che potrebbero instaurarsi fra i pari con l'uso di cellulari e smartphone o delle chat line o social network più diffusi, con particolare riferimento alla prevenzione del cyberbullismo. Sul sito scolastico saranno messi in condivisione materiali dedicati ad alunni e alle famiglie come guide in formato .pdf e video che possono fornire spunti di approfondimento e confronto.

La scuola si impegna alla diffusione delle informazioni e delle procedure contenute nel documento (Policy e-safety) per portare a conoscenza delle famiglie il regolamento sull'utilizzo delle nuove tecnologie all'interno dell'istituto e prevenire i rischi legati a un utilizzo non corretto di internet.

## **3 . Gestione dell'infrastruttura e della strumentazione ICT della scuola.**

Le sedi dell'Istituto sono connesse ad Internet tramite wireless e LAN. La rete didattica è separata dalla rete dell'amministrazione.

**- Accesso a internet: filtri, antivirus e sulla navigazione.**

L'accesso a internet è possibile e consentito per la didattica nei laboratori multimediali. Solo il docente dalla propria postazione può consentire agli alunni di accedere a internet. Le postazioni non sono dotate di webcam. L'accesso è per tutti schermato da filtri che dal server impediscono il collegamento a siti appartenenti a black list o consentono il collegamento solo a siti idonei alla didattica, secondo le impostazioni date dall'Animatore digitale o dall'Assistente Tecnico che periodicamente provvede alla manutenzione e aggiornamento del sistema informatico del laboratorio, ove necessario richiedendo l'intervento di tecnici esterni. Le postazioni degli alunni (client) sono occasionalmente utilizzate anche dai docenti, quando questi si servono dei laboratori. I docenti hanno piena autonomia nel collegamento ai siti web.

**- Gestione accessi (password, backup, ecc.)**

L'accesso al sistema informatico per la didattica e la connessione alla rete wireless è consentito al personale docente attraverso l'assegnazione di una password. La password è personale e consente di accedere al server. Non vi è un backup dei file elaborati, se non quello operato dai docenti interessati sui supporti rimovibili personali. Le postazioni del laboratorio funzionano come stazioni di lavoro e non come archivi.

Tutte le aule sono dotate di dispositivi per la compilazione del registro elettronico e come supporto alla didattica.

Agli studenti è fatto divieto di usare i dispositivi d'aula senza la supervisione dei docenti.

**- E-mail**

L'account di posta elettronica è solo quello istituzionale utilizzato ordinariamente dagli uffici amministrativi., sia per la posta in ingresso che in uscita. L'eventuale invio o ricevimento di posta a scopi didattici avverrebbe solo su autorizzazione del Dirigente scolastico e operativamente sarebbe svolto dall'assistente amministrativo addetto. La posta elettronica è protetta da antivirus, e quella certificata anche dall'antispam.

**- Sito web della scuola**

Il sito dell'Istituto è raggiungibile all'indirizzo [www.liceocanicatti.edu.it](http://www.liceocanicatti.edu.it). Il Dirigente, il Referente del sito ed eventuali altri amministratori in organigramma verificano e aggiornano i contenuti destinati alla pubblicazione.

#### **- Social network**

La scuola mette a disposizione di docenti e alunni la piattaforma didattica Fidenia e promuove e realizza progetti di educazione all'uso consapevole dei social network.

#### **- Protezione dei dati personali.**

Il personale scolastico è "incaricato del trattamento" dei dati personali (degli alunni, dei genitori, ecc.), nei limiti delle operazioni di trattamento e delle categorie di dati necessarie ai fini dello svolgimento della propria funzione e nello specifico della docenza (istruzione e formazione). Tutto il personale incaricato riceve poi istruzioni particolareggiate applicabili al trattamento di dati personali su supporto cartaceo e su supporto informatico, ai fini della protezione e sicurezza degli stessi.

Viene inoltre fornita ai genitori informativa e richiesta di autorizzazione all'utilizzo dei dati personali degli alunni eccedenti i trattamenti istituzionali obbligatori.

### **4. Dispositivi personali e regole per il BYOD**

#### **- Per gli studenti: gestione degli strumenti personali – cellulari, tablet ecc.**

Per gli studenti: è vietato l'utilizzo di cellulari per l'intera durata delle attività scolastiche.

È consentito a tutti gli studenti, in casi specifici concordati con il docente, l'utilizzo di dispositivi elettronici personali per scopi didattici (modalità BYOD, Bring your own device).

Per i docenti: durante l'orario di servizio l'utilizzo di dispositivi elettronici personali è consentito per i soli fini didattici.

Il personale della scuola ha facoltà di usare strumenti personali in caso di stretta necessità o nelle pause di lavoro.

L'azione #6 del Piano Nazionale Scuola Digitale "Politiche attive per il BYOD" (Bring Your Own Device, traduzione: porta il tuo dispositivo) intende garantire a tutti gli studenti una formazione digitale fondata sul saper usare i propri device in modo consapevole.

Nel ribadire che l'uso improprio dei dispositivi digitali mobili a scuola è inaccettabile e sanzionato in base a quanto stabilito dal Regolamento di Istituto, si definiscono, in linea con il PNSD, le seguenti regole BYOD per favorire l'attuazione dell'azione #6, garantendone la sicurezza:

- i dispositivi personali - computer portatili, tablet, e-reader, smartphone - possono essere usati a scuola solo per scopi didattici, previa autorizzazione esplicita dell'insegnante e sotto la supervisione dello stesso
- è severamente vietato usare dispositivi di registrazione audio, videocamere o fotocamere (o dispositivi che li prevedano) per registrare o fare foto in classe senza il permesso dell'insegnante e senza il consenso della persona che viene registrata, videoregistrata, fotografata.
- gli studenti sono personalmente responsabili dei loro dispositivi e della custodia degli stessi
- la scuola non è responsabile della sicurezza dei dispositivi e di eventuali danni o smarrimenti
- agli studenti è richiesto di caricare il dispositivo a casa; non è consentito ricaricare i dispositivi in aula anche per motivi di sicurezza.
- gli studenti devono rispettare la proprietà intellettuale altrui:
  - non sono ammessi copia e/o plagio di qualsivoglia materiale
  - non è ammessa la violazione del copyright
- l'Istituto favorisce e incentiva l'open source e il copyleft
- l'Istituto si riserva il diritto di monitorare le attività online degli utenti e accedere ai contenuti delle stesse, di controllare, copiare, raccogliere o cancellare ogni comunicazione elettronica o file, e di rivellarli ad altri se necessario. L'Istituto può ispezionare, previa autorizzazione anche verbale del genitore o del tutore, la memoria del dispositivo dello studente, se ritiene che le regole non siano state rispettate. Ciò comprende registrazioni audio e video, fotografie scattate negli ambienti di pertinenza dell'Istituto e ogni altro materiale che violi la dignità e la privacy altrui.

**- Per i docenti: gestione degli strumenti personali– cellulari, tablet ecc.**

Durante le ore delle lezioni non è consentito l'utilizzo del cellulare, mentre è consentito l'uso di altri dispositivi elettronici personali solo a scopo didattico ed integrativo di quelli scolastici disponibili.

Durante il restante orario di servizio è consentito l'utilizzo del cellulare solo per comunicazioni personali di carattere urgente mentre è permesso l'uso di altri dispositivi elettronici personali per attività funzionali all'insegnamento, ad integrazione di quelli scolastici disponibili.

**- Per il personale della scuola: gestione degli strumenti personali– cellulari, tablet**

Durante l'orario di servizio al restante personale scolastico è consentito l'utilizzo del cellulare solo per comunicazioni personali di carattere urgente.

## **5. Prevenzione, rilevazione e gestione dei casi a rischio**

## **- Rischi**

I rischi effettivi che si possono correre a scuola nell'utilizzo delle TIC da parte degli alunni derivano da un uso non corretto del telefono cellulare personale o dello smartphone dei pc della scuola collegati alla rete.

Il telefono cellulare o lo smartphone non sono richiesti dalla scuola perché non sono ritenuti indispensabili in ambito scolastico, ma vengono forniti dai genitori degli alunni soprattutto per mantenere la comunicazione diretta con i figli anche fuori dal contesto scolastico. Eludendo la sorveglianza degli insegnanti, attraverso i telefoni cellulari o gli smartphone, dotati di particolari applicazioni e di collegamento a internet, oltre che parlare e scrivere messaggi con i genitori, gli alunni potrebbero anche scaricare e spedire foto personali o intime, proprie o di altri, video con contenuti indecenti o violenti, accedere a internet e a siti non adatti ai minori, ascoltare musica e giocare con i videogiochi non consigliati ai minori, leggere la posta elettronica e comunicare o chattare con sconosciuti, inviare o ricevere messaggi molesti e minacciosi. Eludendo sempre la vigilanza degli insegnanti, gli alunni potrebbero correre gli stessi rischi a scuola anche con l'utilizzo dei pc del laboratorio informatico e con un accesso non controllato a internet.

## **- Azioni**

Le azioni previste di prevenzione nell'utilizzo delle TIC sono le seguenti:

- Informare e formare i docenti, i genitori, il personale ATA e gli studenti sui rischi che un uso non sicuro delle nuove tecnologie può favorire;
- Fornire ai genitori informativa e richiesta di autorizzazione all'utilizzo dei dati personali degli alunni eccedenti i trattamenti istituzionali obbligatori (es. liberatoria per la pubblicazione delle eventuali foto, immagini, testi e disegni relativi al proprio/a figlio/a);
- Non consentire l'utilizzo del cellulare personale degli alunni a scuola, in quanto per assolvere a ogni comunicazione urgente con i genitori o con chi ne fa le veci è sempre disponibile il telefono della scuola supervisionato dal personale addetto al centralino, che prima di passare la telefonata si accerta dell'identità dell'interlocutore;
- Consentire l'utilizzo del cellulare sono in casi particolari ed eccezionali, ad esempio quando ci si trova fuori dal contesto scolastico durante una visita guidata, e comunque sotto la supervisione dell'insegnante, che si accerta preventivamente dell'identità dell'interlocutore;
- Utilizzare filtri, software che impediscono il collegamento ai siti web per adulti (black list);
- Centralizzare il blocco dei siti web sul server del docente, utilizzando software che possono bloccare l'accesso ai siti internet semplicemente esaminando le varie richieste di connessione



provenienti dai client collegati in rete locale, in modo tale che anche indipendentemente dal browser in uso su ciascuna macchina, il software sia capace di intercettare le richieste di collegamento e rigettare quelle che non rispettano le regole imposte dall'amministratore.

Le azioni di contenimento degli incidenti previste sono le seguenti:

- Se la condotta incauta dell'alunno consiste nel fare circolare immagini imbarazzanti, di natura sessuale, su internet, è necessario rimuoverle: contattare il service provider e se il materiale postato viola i termini e le condizioni d'uso del sito chiedere di rimuoverle.
- Se l'alunno viene infastidito od offeso, suggerirgli di modificare i dettagli del proprio profilo sistemandolo su "privato", in modo tale che solo gli utenti autorizzati siano in grado di vederlo (MSN messenger, siti social network, Skype etc.), o suggerirgli di bloccare o ignorare particolari mittenti, di cancellare il loro nominativo dalla lista degli amici con i quali regolarmente chatta, di inserire il compagno o la persona che offende, per quanto riguarda l'e-mail, tra gli indesiderati;
- Consigliare di cambiare il proprio indirizzo e-mail, contattando l'e-mail provider, di scaricare un'applicazione che blocchi chiamate e messaggi da numeri indesiderati o, se necessario, cambiare il numero di cellulare contattando l'operatore telefonico;
- Fare cancellare il materiale offensivo dal telefonino, facendo intervenire i genitori, e chiedere agli studenti di indicare a chi e dove lo hanno spedito per farlo fare anche gli altri, e conservare una copia di detto materiale se necessario per ulteriori indagini;

- Contattare la polizia se si ritiene che il materiale offensivo sia illegale. In caso di foto e video pedopornografici, confiscare il telefonino o altri dispositivi ed evitare di eseguire download, produrne copie, dividerne link o postarne il contenuto, poiché ciò è reato per chiunque.

#### **- Che cosa segnalare**

Gli alunni possono mostrare segni di tristezza o di ansia o di risentimento nei confronti di compagni o di altri e riferire spontaneamente o su richiesta l'accaduto ai docenti. I fatti riferiti possono essere accaduti anche al di fuori della scuola. Anche confrontandosi periodicamente con gli alunni sui rischi delle comunicazioni on-line, i minori possono riferire di fatti o eventi personali o altrui che "allertano" l'insegnante.

Una "prova" di quanto riferito può essere presente nella memoria degli strumenti tecnologici utilizzati, può essere mostrata spontaneamente dall'alunno, può essere presentata da un reclamo dei genitori, può essere notata dall'insegnante che si accorge dell'infrazione in corso. Mentre il docente è autorizzato a controllare le strumentazioni della scuola, per controllare l'uso del telefono cellulare di un alunno si rivolge al genitore.

I contenuti "pericolosi" comunicati/ricevuti a/dai altri, messi/scaricati in rete, ovvero le tracce che possono comprovare l'utilizzo incauto, scorretto o criminoso degli strumenti digitali utilizzabili anche a scuola attualmente dai minori (l'eventuale telefonino/smartphone personale e il pc collegato a Internet) per gli alunni possono essere i seguenti:

- Contenuti afferenti alla privacy (foto personali, l'indirizzo di casa o il telefono, informazioni private proprie o di amici, foto o video pubblicati contro la propria volontà, di eventi privati, ecc.);
- Contenuti afferenti all'aggressività o alla violenza (messaggi minacciosi, commenti offensivi, pettegolezzi, informazioni false, foto o video imbarazzanti, virus, contenuti razzisti, che inneggiano al suicidio, immagini o video umilianti, insulti, videogiochi pensati per un pubblico adulto, ecc.);
- Contenuti afferenti alla sessualità: messaggi molesti, conversazioni (testo o voce) che connotano una relazione intima e/o sessualizzata, foto o video personali con nudità o abbigliamento succinto, immagini pornografiche, foto e video in cui persone di minore età sono coinvolte o assistono ad attività sessuali (pedopornografia), ecc.

### **- Come segnalare: quali strumenti e a chi.**

Per il telefono cellulare ci si può assicurare che l'alunno vittima salvi nel suo telefono ogni messaggio, voce/testo/immagine, conservando così il numero del mittente.

Gli insegnanti, anche con l'ausilio tecnico dell'Animatore digitale, possono provvedere ugualmente a conservare le prove della condotta incauta, scorretta o dell'abuso rilevate sui pc della scuola: soprattutto la data e l'ora, il contenuto dei messaggi e, se possibile, l'ID del mittente (es. username, mail, numero di telefono cellulare) o l'indirizzo web del profilo ed il suo contenuto.

Qualora ci si dovesse accorgere che l'alunno, usando il computer, si sta servendo di un servizio di messaggia istantanea, programma che permette di chattare in linea tramite testo, l'insegnante può copiare, incollare e stampare la conversazione. Per gli eventuali collegamenti non autorizzati a siti social network, video-hosting sites e altri website, l'insegnante può conservare il link, stampare la pagina o salvare la schermata su documento word. Per le e-mail si può stampare la mail o conservare l'intero messaggio, compresa l'intestazione del mittente. Conservare la prova è utile per far conoscere l'accaduto in base alla gravità ai genitori degli alunni, al Dirigente scolastico e per le condotte criminose alla polizia.

Qualora non si disponga di prove, ma solo delle testimonianze dell'alunno, quantunque riferite a fatti accaduti al di fuori del contesto scolastico, le notizie raccolte sono comunque comunicate ai genitori e per fatti rilevanti anche al Dirigente scolastico; e se necessario, anche alla polizia. In particolare, la segnalazione viene fatta a entrambe le famiglie, se oltre alla vittima anche l'autore della condotta negativa è un altro alunno.

Per le segnalazioni di fatti rilevati sono previsti i seguenti strumenti che i docenti possono utilizzare sulla base della gravità dell'accaduto:

- Annotazione del comportamento sul registro e comunicazione scritta ai genitori, che la devono restituire vistata;
- Convocazione scritta e colloquio con i genitori degli alunni, da parte dei docenti;
- Ammonimento del Questore.
- Relazione scritta al Dirigente scolastico.

In base all'urgenza le comunicazioni formali possono essere precedute da quelle informali, effettuate per le vie brevi.

Inoltre, per i reati meno gravi la legge rimette ai genitori degli alunni la scelta di richiedere la punizione del colpevole, attraverso la querela.

Per i reati più gravi (es. pedopornografia) gli operatori scolastici hanno l'obbligo di effettuare la denuncia all'autorità giudiziaria (o più semplicemente agli organi di polizia territorialmente

competenti).

Per i minori autori di atti di cyberbullismo, fra i 14 e i 18 anni, se non c'è querela o denuncia per i reati di cui agli articoli 594, 595 e 612 del codice penale, scatta l'ammonizione: il questore convoca il minore insieme ad almeno un genitore.

La procedura prende il via su sollecitazione della vittima, rappresentata dai genitori o dal tutore, ma può partire anche da terze persone, purché non da una fonte anonima, fino a quando non sia stata presentata la querela o la denuncia. In questi casi si tratta di una misura di prevenzione amministrativa. Le forze dell'ordine, una volta ricevuta l'esposizione dei fatti, trasmettono poi gli atti al questore che convoca il minore autore del reato insieme ad almeno un genitore. Se il questore ritiene sussistente il fatto, assunte le informazioni e sentite le persone informate sui fatti, ammonisce oralmente l'autore dell'atto di cyberbullismo, invitandolo a tenere una condotta conforme alla legge.

In particolare, per i fatti criminosi, ai fini della denuncia, la relazione deve essere redatta nel modo più accurato possibile, indicando i seguenti elementi: il fatto, il giorno dell'acquisizione del fatto nonché le fonti di prova già note e per quanto possibile, le generalità, il domicilio e quant'altro di utile a identificare la persona alla quale il reato è attribuito, la persona offesa, e tutti coloro che sono in grado di riferire circostanze rilevanti per la ricostruzione del fatto.

### *Gestione dei casi*

#### **- Definizione delle azioni da intraprendere a seconda della specifica del caso.**

##### Gestione dei casi di "immaturità"

Può sembrare naturale all'alunno fornire i propri dati sui siti allestiti in modo tale da attrarre l'attenzione dei ragazzi, con giochi e animazioni, personaggi simpatici e divertenti, che richiedono una procedura di registrazione.

Curiosità, manifestazioni di reciproco interesse tra pari, idee e fantasie sulla sessualità sono espressione da una parte del progressivo sviluppo socio-affettivo dell'alunno e dall'altra dei molteplici messaggi espliciti che gli giungono quotidianamente attraverso i media (televisione, DVD, internet, giornali e riviste), i discorsi degli altri bambini o degli adulti.

I comportamenti cosiddetti “quasi aggressivi”, che spesso si verificano tra coetanei, le interazioni animate o i contrasti verbali, o la presa in giro “per gioco”, effettuata anche in rete, mettono alla prova la relazione con i compagni, la supremazia o la parità tra i soggetti implicati e l’alternanza e sperimentazione dei diversi ruoli. Il gruppo dei pari rappresenta anche il momento di conquista dell’autonomia dall’adulto e pertanto luogo di “complicità” e di piccole “trasgressioni”, di scambi “confidenziali” condivisi fra gli amici nella rete o con il cellulare.

Detti comportamenti, che finiscono per arrivare all’attenzione degli adulti, sono controllati e contenuti dai docenti attraverso i normali interventi educativi, di richiamo al rispetto delle regole di convivenza civile e democratica, di rispetto degli altri, per evitare che possano degenerare, diventare pericolosi per sé o offensivi e minacciosi per gli altri.

#### Gestione dei casi di “prepotenza” o “prevaricazione”

I comportamenti definibili “Bullismo” possono esprimersi nelle forme più varie e non sono tratteggiabili a priori, se non contestualizzandoli. Le caratteristiche che aiutano a individuarli e a distinguerli dallo scherzo, dalle intemperanze caratteriali, dai diverbi usuali fra i ragazzi sono la costanza nel tempo e la ripetitività, l’asimmetria (disuguaglianza di forza e di potere), il disagio della/e vittima/e.

Il bullismo si esplica infatti con comportamenti e atteggiamenti costanti e ripetitivi di arroganza, prepotenza, prevaricazione, disprezzo, dileggio, emarginazione, esclusione ai danni di una o più persone, agiti da un solo soggetto, ma in genere da un gruppo.

Nel caso particolare del Cyberbullismo le molestie sono attuate attraverso strumenti tecnologici: invio di sms, messaggi in chat, e-mail offensive o di minaccia;

- diffusione di messaggi offensivi ai danni della vittima, attraverso la divulgazione di sms o e-mail nelle mailing-list o nelle chat-line;
- pubblicazione nel cyberspazio di foto o filmati che ritraggono prepotenze o in cui la vittima viene denigrata.

Il bullismo in particolare può originarsi anche dall’exasperazione di conflitti presenti nel contesto scolastico. Il conflitto, presente in ogni normale intenzione, è da considerarsi come un campanello d’allarme e può degenerare in forme patologiche quando non lo si riconosce e gestisce in un’ottica evolutiva dei rapporti, di negoziazione e risoluzione. Se non gestito positivamente, infatti, il conflitto rischia di mutarsi e provocare effetti distruttivi sulle relazioni (prevaricazione e sofferenza) e sull’ambiente (alterazione del clima del gruppo-classe).

In considerazione dell'età degli alunni considerati possono prefigurarsi alcune forme di interazioni che possono evolvere verso tale fenomeno. Per prevenire e affrontare il bullismo dunque i docenti non solo identificano vittime e prepotenti in divenire, ma tutti insieme affrontano e intervengono sul gruppo-classe, coinvolgendo i genitori degli allievi.

L'elemento fondamentale per una buona riuscita dell'intervento educativo è infatti la corretta, compiuta e convinta ristrutturazione dell'ambiente sociale in cui tale fenomeno si verifica, e in particolare delle relazioni nel contesto della classe. Gli atteggiamenti degli alunni, così come quelli dei loro genitori, possono giocare un molto significativo nel ridurre la dimensione del fenomeno. Gli interventi mirati sul gruppo classe sono gestiti in collaborazione dal team dei docenti della classe e d'intesa con le famiglie - ad esempio con percorsi di mediazione volta alla gestione positiva del conflitto, con gruppi di discussione (circle time), con rappresentazioni e attività di role-play sull'argomento del bullismo, con le strategie del problem solving.

Vengono intrapresi anche i percorsi individualizzati di sostegno alle vittime, volti a incrementarne l'autostima e l'assertività e a potenziare le risorse di interazione sociale, mentre i prevaricatori sono destinatari di interventi mirati a smuoverne le competenze empatiche e a favorire una loro condivisione delle norme morali.

Anche in relazione alle manifestazioni socio-affettive fra pari, al linguaggio sessualizzato o "volgare", al fine di evitare prevaricazioni e imbarazzo o disagio, i docenti intervengono per favorire nei bambini un buon rapporto con il proprio corpo e per far percepire meglio eventuali violazioni dei limiti di prossimità o di "confidenza" ed imparare ad opporvisi, per far acquisire fiducia nelle proprie sensazioni e nel proprio intuito e determinazione nel rifiutare i contatti anche "a distanza" sgradevoli o "strani", per rendere consapevoli gli alunni del diritto al rispetto dei propri limiti e di quelli altrui, per far capire ai ragazzi che l'interazione on-line deve sottostare a delle regole di buon comportamento, né più né meno della comunicazione a viso aperto, quale quella della vita reale.

Inoltre, la scuola, qualora rilevi una situazione psico-socio-educativa particolarmente problematica, convoca i genitori o gli esercenti la potestà per valutare con loro a quali risorse territoriali possono rivolgersi. Consigliata altresì di servirsi dello sportello di ascolto psicologico gratuito se attivo presso la scuola. Promuove e supporta la richiesta delle famiglie rivolta ai Servizi Sociali dell'Ente Locale per la fruizione di servizi socio-educativi comunali e alla ASL per quanto di competenza psicologica e psicoterapeutica (Pediatria, Neuropsichiatria infantile, Consultorio Familiare).

### Gestione degli "abusi sessuali"

“In generale si parla di abuso sessuale sui bambini quando un minore viene coinvolto in un atto sessuale. Ciò è caratterizzato dal fatto che il minore potrebbe non comprendere del tutto tale atto, non è informato e quindi non è in grado di acconsentire, oppure sulla base del suo livello di sviluppo non è ancora pronto per tale atto e non può dare il proprio consenso”.

Lo spettro delle forme di abuso e di violenza è diventato ancora più ampio e subdolo in seguito alle possibilità offerte dai nuovi mezzi di comunicazione come internet, il cellulare o altri dispositivi tecnologici, e il loro utilizzo sempre più diffuso non fa che acuire il problema. Internet, infatti, permette di scaricare o vendere immagini o filmati di pornografia infantile.

Succede sempre più frequentemente che un adulto prenda contatto con dei minori nei forum o nelle chat su internet, e che li metta di fronte a domande o messaggi sessuali o addirittura a immagini pornografiche.

La denuncia all'autorità giudiziaria o agli organi di Polizia, da parte degli insegnanti o del Dirigente scolastico, costituisce il passo necessario per avviare un intervento di tutela a favore della vittima e attivare un procedimento penale nei confronti del presunto colpevole.

La presa in carico di situazioni di abuso sessuale, così delicate e complesse, richiede un approccio multidisciplinare, da parte di diverse figure professionali. I versanti su cui si articola l'intervento possono essere essenzialmente tre: medico, socio-psicologico e giudiziario.

Il compito della scuola non è comunque solo quello di “segnalare”, ma più ampio ed importante, soprattutto nella prevenzione dell'abuso, nonché nella ripresa della piccola vittima, in quanto ha al suo interno fattori relazionali ed educativi che possono aiutare il bambino a riprendere una crescita serena.

A tal fine la scuola lavora insieme alle altre figure professionali e alle famiglie, scambiando informazioni e condividendo progetti e prassi operative, favorendo le occasioni di confronto e di dialogo.

## ***UTILIZZO DEL LABORATORIO DI INFORMATICA, DELLE POSTAZIONI DI LAVORO E DELL' UTILIZZO DI INTERNET***

### **Disposizioni sull'uso del laboratorio**

1. Le apparecchiature presenti nella scuola sono un patrimonio comune, quindi, vanno utilizzate con il massimo rispetto.
2. I laboratori informatici e le postazioni informatiche dell'istituto possono essere utilizzati esclusivamente per attività di insegnamento, funzionali all'insegnamento e di formazione del personale docente e non docente.
3. Quando un insegnante, da solo o in classe, usufruisce del laboratorio deve obbligatoriamente registrare il proprio nome e l'eventuale classe nell'apposito registro delle presenze di laboratorio, indicando l'orario di ingresso, quello di uscita e motivazione dell'uso delle postazioni informatiche. Questo allo scopo di poter risalire alle cause di eventuali inconvenienti o danneggiamenti e per comprovare l'effettivo utilizzo dell'aula.
4. L'ingresso degli allievi nei laboratori è consentito solo in presenza dell'insegnante.
5. Il docente accompagnatore è responsabile del corretto uso didattico di hardware e software.
6. Nei laboratori è vietato utilizzare CD personali o dischetti se non dopo opportuno controllo con sistema di antivirus aggiornato.
7. È vietato cancellare o alterare files-dati presenti sull'hard disk.
8. Il laboratorio non deve mai essere lasciato aperto o incustodito quando nessuno lo utilizza. All'uscita dal laboratorio sarà cura di chi lo ha utilizzato lasciare il mobilio in ordine, le macchine spente correttamente (chiudi sessione...).
9. In caso di malfunzionamento o guasto dei computer bisogna darne tempestiva segnalazione al responsabile del laboratorio.
10. In caso di malfunzionamento non risolvibile dal responsabile di laboratorio si contatterà personalmente o attraverso il Responsabile di laboratorio, la segreteria.
11. Per motivi di manutenzione straordinaria, in caso di guasti o di virus, i PC possono essere formattati senza preavviso. Si consiglia pertanto di salvare i dati importanti su Cd o pen drive periodicamente.



## **Disposizioni sull'uso dei software**

1. I software installati sono ad esclusivo uso didattico.
2. In base alle leggi che regolano la distribuzione delle licenze, i prodotti software presenti in laboratorio non sono disponibili per il prestito individuale. Nei casi in cui lo fossero in base a precise norme contrattuali i docenti interessati, dopo aver concordato il prestito con il Responsabile di laboratorio, devono compilare l'apposito registro di consegna software custodito in laboratorio.
3. È fatto divieto di usare software non conforme alle leggi sul copyright. E' cura dell'insegnante utente di verificarne la conformità. Gli insegnanti possono installare nuovo software sui PC del laboratorio previa autorizzazione del Responsabile di laboratorio e/o dell'Assistente Tecnico. Si raccomanda, quindi, di verificare che il software installato rispetti le leggi sul copyright.
4. E' responsabilità degli insegnanti che chiedono al Responsabile di laboratorio di effettuare copie di cd/dvd per uso didattico, di assicurarsi che la copia non infranga le leggi sul copyright in vigore.

## **Accesso a internet**

- 1) L'accesso a Internet è consentito al personale docente e non docente solo ad esclusivo uso didattico e/o di formazione e alle classi accompagnate e sotto la responsabilità di un insegnante;
- 2) Internet non può essere usato per scopi vietati dalla legislazione vigente;
- 3) L'utente è direttamente responsabile, civilmente e penalmente, a norma delle vigenti leggi, per l'uso fatto del servizio Internet;
- 4) E' vietato inserire sui pc connessi in rete programmi contenenti virus, scaricare software non autorizzati da internet, scaricare e installare software senza licenza.

## **Norme finali**

Il Responsabile di laboratorio che verifichi un uso del laboratorio contrario a disposizioni di legge o del regolamento interno deve darne comunicazione per iscritto al Dirigente Scolastico.

**AD INTEGRAZIONE DEL PATTO EDUCATIVO DI  
CORRESPONSABILITA' SCUOLA-FAMIGLIE PER AZIONI DI  
PREVENZIONE DEL BULLISMO E DEL CYBERBULLISMO E  
ED UN USO CORRETTO DEI DISPOSITIVI DIGITALI, SOCIAL  
MEDIA E CHAT DA PARTE DEI MINORI  
(ai sensi della L. 71 del 18/6/2017 )**

L'Istituto, pur vietando l'uso del cellulare a scuola, prevede l'utilizzo delle Tecnologie per fini didattici ed ha regolamentato tali utilizzi nei documenti caratterizzanti l'azione didattico-educativa (PTOF, E-Safety Policy, Regolamento d'Istituto, Regolamenti di disciplina) ritiene tuttavia che **Scuola e Genitori** debbano stringere un **patto educativo-collaborativo** perché i minori vengano resi consapevoli sulle conseguenze di un uso scorretto dei dispositivi digitali, dei social-media, delle chat e del Web.

L'Istituto, in piena sintonia con quanto espresso nei Regolamenti caratterizzanti la tematica, con quanto stabilito dal *Regolamento delle studentesse e degli studenti* e a seguito, infine, dell'emanazione della L. 71 del 18/6/2017 *Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo*,

**PROPONE**

il seguente **Patto educativo di corresponsabilità**, affinché, insieme, la Scuola e i Genitori si adoperino per far comprendere ai ragazzi che se le potenzialità della rete vengono mal gestite le conseguenze sul piano psicologico, civile e penale nonché economico, potrebbero essere molto gravi. Ciò vale anche quando certi comportamenti sono attuati fuori dall'orario scolastico e dalla scuola, con gravi ricadute nel contesto scolastico stesso.

Pertanto si chiede che

**LA FAMIGLIA SI IMPEGNI A VIGILARE PER UN USO CORRETTO DI SMARTPHONE, DISPOSITIVI DIGITALI ED INTERNET A CASA ATTRAVERSO ALCUNE SEMPLICI AZIONI PREVENTIVE, QUALI:**

**Mostrarsi coinvolti**: chiedendo al proprio figlio/a di spiegare come vengono usati i dispositivi tecnologici e digitali a scuola per lo svolgimento delle lezioni, per scaricare materiali didattici e per presentare attività e/o lavori individuali e di gruppo sotto la guida dell'insegnante.

**Sottolineare ciò che si ritiene inaccettabile** (razzismo, violenza, linguaggio volgare, pornografia), discutendo sul criterio con cui bisogna selezionare/scaricare file e della possibilità di ricevere file con virus.

**Raccomandare** di non scaricare file da siti sconosciuti.

**Incoraggiare** il proprio figlio/a a comunicare alla famiglia, o eventualmente a un docente di cui ha fiducia, la visione di immagini particolari o la ricezione di e-mail indesiderate.

**Incoraggiare** il proprio figlio/a a confidarsi con la famiglia o con un docente di cui ha fiducia in caso sia stato oggetto di comportamenti vessatori/adescamenti.

- **Discutere sulle conseguenze** che potrebbero esserci se il proprio figlio/a visita sia deliberatamente che involontariamente siti non adatti, guidandolo a comprendere come evitare azioni informatiche sbagliate.
- **spiegare 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; in caso contrario vanno periodicamente cambiati.
- **Spiegare** che non tutti in Internet sono **chi** realmente dichiarano di essere; di conseguenza i ragazzi non dovrebbero mai accordarsi per appuntamenti senza il consenso della famiglia.
- **Denunciare alle Autorità competenti**, sentita la Scuola, eventuali azioni vessatorie subite dai figli, continuate nel tempo e lesive della dignità personale.

I genitori comunque rispondono per gli episodi commessi dai figli minori a titolo di **culpa in educando** (articolo 2048 del Codice civile). Sono esonerati da responsabilità solo se dimostrano di non aver potuto impedire il fatto. Ma nei casi più gravi per i giudici l'inadeguatezza dell'educazione impartita ai figli emerge dagli stessi episodi di bullismo, che per le loro modalità esecutive dimostrano maturità ed educazione carenti. Il Tribunale di Alessandria (sentenza 439 del 16 maggio 2016), nel caso di un filmato girato da un gruppo di studenti e poi diffuso in rete, ha riconosciuto la responsabilità anche dei genitori del minore che non ha effettuato materialmente il video, ma che non si è dissociato dall'azione.

**L'ISTITUZIONE SCOLASTICA S'IMPEGNA A DICHIARARE, IN APPOSITO DOCUMENTO, LE AZIONI DI PREVENZIONE E DI CONTRASTO AL BULLISMO ED AL CYBERBULLISMO E AD ATTUARLE ATTRAVERSO:**

- **l'adozione del documento di Esafety Policy** come previsto della Legge 71/18.6.2017 su *Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo*;
- **l'assunzione di responsabilità**, rispetto alla quale i docenti devono svolgere con diligenza gli obblighi di vigilanza e sorveglianza costante; ad esempio anche impedendo, in orario scolastico, la ripresa fotografica o la registrazione di video non correlati ai fini didattici; avvisando il dirigente e i genitori degli alunni coinvolti e attuando le procedure preventive e/o sanzionatorie previste dai Regolamenti interni.
- **l'informazione alle componenti scolastiche**, che tutti coloro che hanno preso parte all'episodio di bullismo o cyberbullismo, a prescindere dal ruolo svolto, hanno **una responsabilità solidale** (sentenza della Cassazione n. 20192 del 25 settembre 2014); e che, anche se il cyberbullismo in sé non è reato, la legge colpisce le singole condotte agite quali: **diffamazione aggravata** (articolo 595, comma 3, Codice penale), **trattamento illecito dei dati personali** (articolo 167, Dlgs 196/2003), **violenza privata** (articolo 610 Codice penale) o **lesioni** (articoli 581 e 582 Codice penale), **percosse, fino al reato di stalking** (articolo 612-bis Codice penale).
- **la formazione di tutti gli operatori scolastici sul fenomeno del bullismo e del cyberbullismo**, in particolare su quest'ultimo per il quale si intendono: *“ gli atti reiterati e vessatori commessi, spesso da minorenni contro altri minorenni, attraverso Internet, in grado di ingenerare nella vittima un forte disagio e nei casi più gravi anche gesti di autolesionismo o istigazione al suicidio”*. In genere, la condotta si manifesta con la diffusione in rete di video e post offensivi, che si diffondono in modo “virale”;

- **l'azione di denuncia della Scuola alle Autorità competenti**: dei fatti accaduti; anche perché a volte identificare i cyberbulli può risultare complesso: l'autore può cambiare in continuazione indirizzo Ip, tornando online subito dopo l'oscuramento tramite il sequestro preventivo

## **Modulistica allegata**

MODULO DI RICHIESTA DI CREDENZIALI DI AUTENTICAZIONE PER L'ACCESSO  
AD INTERNET NELLA RETE DI ISTITUTO

Al Dirigente Scolastico  
dell'Istituto Istruzione Superiore "Foscolo"

Il/La sottoscritto/a \_\_\_\_\_, nato/a a \_

(\_\_\_\_), il \_\_\_\_\_, residente a \_

in via \_\_\_\_\_, n. \_\_\_\_\_ CAP \_

codice fiscale \_\_\_\_\_, email \_\_\_\_\_

in qualità di:

- studente
- personale dell'Istituto

**chiede il rilascio delle credenziali di autenticazione per l'accesso ad Internet tramite la rete wireless o cablata dell'Istituto.**

Dichiara di essere consapevole delle implicazioni di responsabilità personale derivanti dall'accesso alla rete internet e dagli eventuali abusi.

In particolare si impegna a:

- non scaricare/duplicare/distribuire software o altri contenuti protetti da diritto d'autore;
- non accedere a siti o risorse dal contenuto illegale o non consono alle regole di comportamento dettate dal carattere istituzionale ed educativo della scuola (ad esempio, siti con contenuto violento, pedo-pornografico, razzista, etc...);
- non diffondere virus o altri software malevoli all'interno della rete e a dare immediato avviso all'Amministrazione della Rete di comportamenti anomali o di infezioni riconosciute;
- conservare le proprie credenziali di accesso alla rete in modo scrupoloso, non comunicandole ad altre persone. E' bene ricordare che l'accesso attraverso l'autenticazione trasferisce direttamente la responsabilità degli atti commessi durante la navigazione all'intestatario delle credenziali stesse.

Altre notifiche:

- In caso di accesso con un proprio dispositivo, l'Istituto non potrà essere ritenuto in alcun modo responsabile per eventuali danni legati alla fruizione del servizio di rete, ivi comprese le infezioni da virus o altri software malevoli.
- L'accesso alla rete wireless non è garantito e può subire limitazioni, sospensioni, blocchi, dipendenti o meno dalla volontà dell'Istituto. In nessun caso l'utente potrà rivalersi sull'Istituto per il mancato servizio.
- Il servizio wireless viene fornito con limitazioni definite sul numero di accessi contemporanei, in modo che potranno verificarsi situazioni di sovraccarico della rete e conseguente disconnessione o mancata connessione dei client.
- L'autorizzazione all'uso della rete di Istituto potrà venire revocata (cancellazione dell'utente) in qualsiasi momento per cause tecniche o per motivazioni legate all'uso improprio o alla violazione delle norme di comportamento.
- E' disponibile un servizio di assistenza alla connessione, contattando l'Amministratore di Rete o uno dei Tecnici dell'Istituto.

Data \_\_\_\_\_

Firma leggibile \_

**- Procedure operative per la protezione dei dati personali.**

DICHIARAZIONE LIBERATORIA DEI GENITORI/TUTORI PER LA PUBBLICAZIONE  
DI ELABORATI, NOMI, VOCI, IMMAGINI, MATERIALE AUDIOVISIVO

Al Dirigente Scolastico  
dell'Istituto Istruzione Superiore "Foscolo"

**Oggetto: Liberatoria per l'utilizzo delle immagini.**

- Dati dell'Alunno

Cognome \_\_\_\_\_ Nome \_\_\_\_\_ nato/a

\_\_\_\_\_ il \_\_\_\_\_

Scuola \_\_\_\_\_ classe \_\_\_\_\_ sez. \_\_\_\_\_

\_\_\_\_\_.

- Dati del genitore

\_L\_ sottoscritt \_\_\_\_\_

con la presente

**AUTORIZZA**

l'utilizzo delle immagini registrate nell'ambito delle attività/progetti realizzati dall'istituzione Scolastica, con diffusione sulle piattaforme digitali e in televisione, nel pieno rispetto della funzione educativa degli interventi. La posa e l'utilizzo delle immagini sono da considerarsi effettuate in forma gratuita.

Firma del genitore

\_\_\_\_\_

**-Istanza di ammonimento al Questore**

Al Signor Questore di

\_\_\_\_\_  
\_\_\_\_\_

**Istanza di ammonimento**

Il sottoscritto \_\_\_\_\_ Luogo di nascita \_\_\_\_\_  
\_\_\_\_\_ Residenza \_\_\_\_\_ Recapiti \_\_\_\_\_  
\_\_\_\_\_

non avendo ancora sporto querela per i fatti di seguito narrati,

**CHIEDE**

Che la S.V. proceda all'ammonimento nei confronti di \_\_\_\_\_

Poiché, con le proprie reiterate condotte qui di seguito esposte, ha ingenerato nell'istante uno stato di grave e perdurante ansia, fino all'induzione a temere per la propria incolumità, costringendo l'istante, altresì, ad alterare radicalmente le proprie abitudini di vita.

I fatti persecutori che spingono l'istante a chiedere l'ammonimento della persona indicata sono i seguenti: \_\_\_\_\_

Pertanto, si chiede che la S.V. proceda all'ammonimento nei confronti di: \_\_\_\_\_

Luogo di nascita: \_\_\_\_\_ Data di nascita: \_\_\_\_\_

Residenza: \_\_\_\_\_

Atteso che la reiterazione di tali comportamenti costituisce un aggravamento della situazione attuale che già allo stato appare intollerabile per chi scrive.

L'istante, per i motivi sopra narrati, ribadisce la propria volontà affinché la S.V. proceda all'ammonimento nei confronti di \_\_\_\_\_

\_\_\_\_\_ li, \_\_\_\_\_

In fede