



ISTITUTO D'ISTRUZIONE SUPERIORE  
"GIUDICI SAETTA E LIVATINO"

Con sezioni associate Liceo Scientifico - Liceo Scienze Umane  
I.T.C. "Gino Zappa" (Campobello di Licata)

Viale Lauricella, 2 - 92029 Ravanusa (AG) Tel.0922/875745 Fax 0922 874018

## ***E-SAFETY POLICY***

*(documento coerente con la Legge 71/2017)*

### **1 INTRODUZIONE**

#### **1.1. Scopo della Policy**

Nel corso dell'a.s. 2020-21 questa Istituzione scolastica ha redatto e pubblicato il seguente documento di e-policy che raccoglie le linee di condotta, le norme comportamentali da seguire per promuovere un utilizzo consapevole e corretto della rete, più in generale delle TIC all'interno del contesto scolastico.

Tale documento va assunto come una guida, che si propone di:

- descrivere le norme comportamentali e le procedure per l'utilizzo delle ICT in questo Istituto, le misure per la prevenzione e quelle per la rilevazione e gestione delle problematiche connesse a un uso non consapevole delle tecnologie digitali.
- prevenire fenomeni legati ai rischi delle tecnologie digitali;
- segnalare i casi individuati all'interno della scuola;
- gestire i casi, ovvero le misure che la scuola intende attivare a supporto delle famiglie e degli studenti vittime o spettatori attivi e/o passivi di quanto avvenuto.

#### **1.2. Integrazione della Policy con Regolamenti esistenti.**

Il documento integra per obiettivi e contenuti i documenti che specificano le politiche dell'Istituto :

- PTOF, incluso il piano per l'attuazione del PNSD;
- RAV Rapporto di autovalutazione

- Regolamento interno d'istituto;
- il Regolamento per l'utilizzo dei laboratori di informatica

## 2. IL DOCUMENTO E- POLICY

### + A) Ruoli e responsabilità

#### + Dirigente scolastico:

- garantire la tutela degli aspetti legali riguardanti la privacy e la tutela dell'immagine di tutti i membri della comunità scolastica;
- garantire ai propri docenti una formazione di base sulle Tecnologie dell'Informazione e della Comunicazione (ICT) che consenta loro di possedere le competenze necessarie all'utilizzo di tali risorse;
- garantire l'esistenza di un sistema che consenta il monitoraggio e il controllo interno della sicurezza online;
- deve informare tempestivamente, qualora venga a conoscenza di atti di cyberbullismo che non si configurino come reato, i genitori dei minori coinvolti (o chi ne esercita la responsabilità genitoriale o i tutori)
- Il dirigente Scolastico regola il comportamento degli studenti ed impone sanzioni disciplinari in caso di comportamento inadeguato.

#### + Referente cyberbullismo d'Istituto:

- Coordina iniziative di prevenzione e contrasto del cyberbullismo messe in atto dalla scuola;
- Predisporre un documento di rilevazione di incidenti di sicurezza in rete;
- Facilita la formazione e la consulenza di tutto il personale;
- Raccoglie e diffonde buone pratiche educative, organizzative e azioni di monitoraggio
- Favorisce l'elaborazione di un modello di e-policy d'istituto
- Collaborare in team con altre figure scolastiche (animatore digitale-referente)
- BES /Inclusione - psicologo scolastico – referente per la dispersione

etc...

- Segnalazioni situazione di rischi on line o casi di bullismo e cyberbullismo;
- Supporta gruppi di lavoro per la modifica di documenti scolastici e predisposizione di linee guida.

#### **+ Animatore Digitale e Team dell'Innovazione:**

- Pubblicano il documento di E-Safety Policy sul sito della scuola;
- Diffondono i contenuti del documento PNSD tra docenti e studenti.

#### **+ Insegnanti:**

- provvedono personalmente alla propria formazione/aggiornamento sull'utilizzo del digitale con particolare riferimento alla dimensione etica (tutela della privacy, rispetto dei diritti intellettuali dei materiali reperiti in Internet e dell'immagine degli altri: lotta al cyberbullismo);
- supportano gli alunni nell'utilizzo consapevole delle tecnologie informatiche utilizzate a scopi didattici;
- segnalano al referente situazioni o problematiche verificatesi di cui vengono a conoscenza o hanno sentore;
- segnalano al Dirigente scolastico e ai suoi collaboratori eventuali episodi di violazione delle norme di comportamento stabilite dalla scuola, avviando le procedure previste in caso di violazioni;
- supportano ed indirizzano alunni coinvolti in problematiche legate alla rete;
- informano i genitori eventuali problematiche emerse in classe nell'utilizzo del digitale, e stabiliscono comuni linee di intervento per affrontarle;

#### **+ Alunni:**

- leggono, comprendono ed accettano il documento di E-Safety Policy;
- comprendono e rispettano le norme sul diritto d'autore;
- acquisiscono le indicazioni per un uso corretto e responsabile delle ITC, attuando le regole del e-safety, per evitare situazioni di rischio;
- devono avere consapevolezza delle situazioni di rischio legate alla rete, telefoni cellulari, fotocamere digitali;
- devono conoscere la politica della scuola sull'uso delle immagini;
- comprendono l'importanza di adottare buone pratiche di sicurezza on-line quando si usano le tecnologie;

- si assumono la responsabilità di un utilizzo sbagliato delle tecnologie.

#### ✚ **Tecnico informatico:**

- può controllare ed accedere a tutti i file dell'intranet;
- è l'unico a poter installare nuovo software;
- limita attraverso un proxy l'accesso ad alcuni siti;
- la prenotazione dei laboratori consente di tenere traccia di ora e laboratorio utilizzati da ciascuno.

#### ✚ **Direttore dei Servizi Generali e Amministrativi:**

- assicura, nei limiti delle risorse finanziarie disponibili, gli interventi di manutenzione necessari ad evitare un cattivo funzionamento della dotazione tecnologica dell'Istituto, controllando al contempo che le norme di sicurezza vengano rispettate;

#### ✚ **Genitori:**

- contribuiscono, in sinergia con il personale scolastico, alla sensibilizzazione dei propri figli sul tema della sicurezza in rete;
- incoraggiano l'impiego delle ICT da parte degli alunni nello svolgimento dei compiti a casa, controllando che tale impiego avvenga nel rispetto delle norme di sicurezza;
- agiscono in modo concorde con la scuola per la prevenzione dei rischi e l'attuazione delle procedure previste in caso di violazione delle regole stabilite;
- rispondono per gli episodi commessi dai figli minori a titolo di colpa 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.

### **3) SANZIONI PER VIOLAZIONE DEL POLICY**

**Premesso che le sanzioni disciplinari si baseranno sul principio di gradualità commisurato alla gravità delle violazioni commesse, si prevedono le seguenti:**

- richiamo verbale;
- sanzioni estemporanee (assegnazione di attività aggiuntive da svolgere a casa su temi di Cittadinanza e Costituzione);
- sospensione dalle lezioni
- privazione della partecipazione a progetti, viaggi di istruzione o altre attività alternative;
- nota informativa ai genitori o tutori mediante registro elettronico;
- convocazione dei genitori o tutori per un colloquio con l'insegnante;
- convocazione dei genitori o tutori per un colloquio con il Dirigente scolastico.

**Nei casi di comportamenti configurabili come ipotesi di reato verrà informata l'autorità giudiziaria di competenza**

## **4 CURRICOLO E FORMAZIONE**

### **4.1. Curricolo sulle competenze digitali per gli studenti**

Nell'ambito del PNSD l'Istituto si può proporre un programma di educazione alla sicurezza on-line da affiancarsi ad una didattica digitale.

- Promuovere una serie di comportamenti "adeguati":
- Appurare l'attendibilità delle informazioni trovate in rete;
- Riportare sempre la fonte delle informazioni pervenute;
- Conoscere e rispettare la netiquette (regole condivise che disciplinano il rapporto tra utenti della rete, siti e qualsiasi altro tipo di comunicazione);
- Mantenere private le informazioni personali proprie e degli altri;
- Comprendere che le fotografie in rete possono essere manipolate o utilizzate per scopi diversi da quelli per cui sono state pubblicate;
- Comprendere che la rete traccia e tiene memoria di tutto ciò che viene pubblicato;
- Comprendere il motivo per cui non bisogna pubblicare foto o video di altre persone senza il loro consenso;
- Conoscere le conseguenze di azioni sbagliate in rete;
- Conoscere le diverse forme di cyberbullismo e le persone e/o associazioni a cui rivolgersi per chiedere consiglio;

- Rispettare i copyright.

## 4.2. Formazione dei docenti sull'utilizzo consapevole e l'integrazione delle TIC nella didattica

Le attività di formazione si possono svolgere su diversi livelli:

- formazione istituzionale, organizzata dal Miur secondo il PNSD, attraverso gli snodiformativi;
- formazione istituzionale in contrasto al bullismo, attraverso:
  - interventi su classi individuate dalla scuolastessa,
  - interventi che vedono la presenza dell'intera comunità educante, compresi i genitori,
  - la formazione dei referenti di istituto;
  - formazione specifica di Istituto, legata alle esigenze formative rilevate;
  - partecipazione a progetti internazionali con la finalità di condividere materiale e tecniche di prevenzione e gestione di casi di bullismo per possibilità di costruire una conoscenza collaborativa con altri paesi attraverso la piattaforma e-twinning .

## 4.3. Sensibilizzazione delle famiglie

Il presente documento verrà pubblicato sul sito ed affiancato da un vademecum per i genitori affinché comprendano i rischi della rete e collaborino proficuamente con il personale della scuola.

I progetti realizzati dagli studenti verranno pubblicati sul sito della scuola nella giornata mondiale della sicurezza in rete al fine di mettere in evidenza e valorizzare il contributo degli studenti

Seguire i consigli della campagna europea contro il bullismo (<http://www.e-abc.eu/it/bullismo/>)

#### 4.4. Gestione dell'infrastruttura e della strumentazione ICT della scuola.

##### 4.4.1. Gestione accessi (password, backup, ecc.)

Nei computer presenti nei laboratori sono previsti diversi profili di accesso con password relative:

- amministratore;
- docente;
- classe;
- guest.

##### 4.4.2 Sito web della scuola

La scuola ha un sito web nel quale sono pubblicati tutti i documenti relativi la sicurezza in rete e la prevenzione di rischi legati ad un uso inconsapevole o sbagliato della stessa.

##### 4.4.3. Socialnetwork

L'istituto ha una pagina Facebook per la pubblicazione di eventi o attività della scuola.

## 5. BYOD

### 5.1 Per gli studenti: gestione degli strumenti personali - cellulari, tabletecc..

Come espresso nel Patto di corresponsabilità, gli alunni si impegnano a tenere spenti e custoditi in cartella i telefoni cellulari a meno che non siano utili per scopi didattici

### 5.2 Per i docenti: gestione degli strumenti personali - cellulari, tabletecc..

Durante le ore di lezione è consentito ai docenti l'uso di dispositivi elettronici personali, come il tablet, unicamente a scopo didattico e a integrazione dei dispositivi scolastici disponibili.

### 5.3. Per il personale della scuola: gestione degli strumenti personali - cellulari, tabletecc..

L'uso di dispositivi elettronici personali è permesso solo per attività funzionali al servizio

## 6. PREVENZIONE, RILEVAZIONE E GESTIONE DEI CASI

### 6.1 Prevenzione

#### Gestione del rischio: RESPONSABILITÀ

- (docenti) riconoscere i rischi più comuni che i ragazzi possono correre sul web, per potere poi intervenire adeguatamente.
- Monitorare situazioni (Referente-Docenti- Personale scolastico)
- Attuare percorsi scolastici di educazione all'affettività, educazione alla cittadinanza ed alla convivenza civile, educazione al rispetto, educazione all'uso consapevole della rete, incontri con istituzioni
- catalogare e illustrare le tipologie di cyberbullismo
- Flaming: è l'atto di inviare deliberatamente un messaggio ostile e provocatorio
- Sexting: invio di foto o video a sfondo sessuale
- Harassment: come il primo caso, ma i messaggi sono esclusivamente diretti alla vittima
- Denigration: insultare mettendo in giro voci e pettegolezzi spesso inventati
- Exclusion: far sentire solo qualcuno, isolandolo dal gruppo
- Cyberstalking: persecuzione online incessante
- Impersonation: furto di identità
- Tricky o Outing: il cyberbullo pubblica online a nome altrui informazioni imbarazzanti (furto identità)
- Integrare il curriculum d'istituto con progetti
- Informare famiglie e comunità: PTOF, RAV, PdM, Regolamento istituto, Bilancio sociale

### 6.2. AZIONI:

avviare azioni di contrasto efficaci e mirate, rispetto ai rischi sopra elencati.

(Tra le azioni utili a contrastare i rischi derivanti da un utilizzo improprio dei dispositivi digitali da parte degli studenti in orario scolastico, possono suggerirsi le seguenti:

- diffondere un'informazione adeguata al personale scolastico, agli studenti e alle famiglie, sui rischi che i minori possono correre sul web;

introdurre regole precise per l'uso di dispositivi digitali propri,



quali cellulare e smartphone, agli studenti in orario scolastico, regolamentando l'uso del cellulare e la supervisione diretta di un docente responsabile;

- dotare i dispositivi della scuola di filtri che impediscano l'accesso a siti web non adatti ai minori (blacklist);
- osservare le fasce orarie (08:00 -18:00) in conformità al diritto alla disconnessione (CCNL 2016/2018).

### 6.3. Rilevazione e denunce

#### 6.3.1. Che cosa segnalare

andranno opportunamente segnalati:

- dati particolari o riservati pubblicati in chat o social network (foto, immagini, video personali, informazioni private proprie e di amici; l'indirizzo di casa o il telefono, ecc.);
- contenuti che possano considerarsi in qualche modo lesivi dell'immagine altrui (commenti offensivi, minacce, osservazioni diffamatorie o discriminatorie, foto o video denigratori, videogiochi che contengano un'istigazione alla violenza, ecc.);
- contenuti irrispettabili alla sfera sessuale: messaggi, immagini o video a sfondo sessuale, come foto di nudo o semi-nudo, ecc.

#### 6.3.2. Come segnalare: quali strumenti e a chi

##### **Docente:**

- Informare il Dirigente scolastico, il referente d'istituto e le famiglie coinvolte in merito all'accaduto ed, eventualmente, la Polizia Postale.

##### **Referente d'istituto:**

Compilazione di un registro per tenere traccia di tutte le segnalazioni e, se necessario, chiedere supporto alle Associazioni territoriali o alla Polizia Postale.

### **6.3.3. Come gestire le segnalazioni.**

Raccogliere la segnalazione dell'alunno/docente/personale scolastico corredata da prove che attestino l'azione avvenuta.

Dare tempestiva informazione delle famiglie in merito all'accaduto, raccogliere testimonianze sui fatti da riferire al Dirigente Scolastico ed, eventualmente, alla Polizia Postale

### **6.4. Gestione dei casi**

**Presa in carico da parte dell'insegnante che può rivolgersi alle seguenti figure:**

- Dirigente scolastico
  - Referente d'istituto
  - Polizia di Stato/ Poliziapostale
  - Telefono azzurro (chat anonima o numero verde 19696)
  - Save the Children
  - Numero verde 800669696 (Ministero della Pubblica Istruzione: campagna "Smonta il bullo")
  - APP youpol
-