MINISTERO DELL'ISTRUZIONE DELL'UNIVERSITÀ E DELLA RICERCA
I.I.S. "A. Panzini"
- Via Capanna 62/A – 60019 Senigallia (AN)
071 791111 anis01900a@istruzione.it

E-Safety Policy

1 Introduzione

1.1. Scopo della Policy

Il presente documento ha lo scopo di descrivere le norme comportamentali e le procedure per l'utilizzo delle ICT nell'Istituto di Istruzione Superiore "A. Panzini", le misure per la prevenzione e quelle per la rilevazione e gestione delle problematiche connesse a un uso non consapevole delle tecnologie digitali.

Grazie a un percorso guidato e al materiale di supporto messo a disposizione sul sito del progetto www.generazioniconnesse.it, si definiscono qui le misure che l'Istituto intende adottare:
a) per **promuovere** l'educazione all'uso consapevole della rete internet e l'educazione ai diritti e ai doveri legati all'utilizzo delle tecnologie informatiche;
b) per la **prevenzione**, ovvero le azioni finalizzate alla prevenzione di fenomeni legati ai rischi delle tecnologie digitali;
c) per la **segnalazione** dei casi, ovvero le disposizioni semplici su come segnalare i casi nella scuola;
d) per la **gestione dei casi**, ovvero le misure che la scuola intende attivare a supporto delle famiglie e degli studenti che sono stati vittime o spettatori attivi e/o passivi di quanto avvenuto.

1.2. Ruoli e responsabilità

1. Dirigente scolastico:
   - garantisce la tutela degli aspetti legali riguardanti la privacy e la tutela dell'immagine di tutti i membri della comunità scolastica;
   - garantisce 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;
   - garantisce l'esistenza di un sistema che consenta il monitoraggio e il controllo interno della sicurezza on line;
   - informa 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)

2. Referente cyberbullismo d'Istituto:
   - coordina delle iniziative di prevenzione e contrasto del cyberbullismo messe in atto dalla scuola;
   - Predispone un documento di rilevazione di incidenti di sicurezza in rete;
   - Facilita la formazione e la consulenza di tutto il personale.

3. Animatore Digitale e Team dell'Innovazione:
   - Pubblicano il documento di E-Safety Policy sul sito della scuola;
   - Diffondono i contenuti del documento tra docenti e studenti.

4. 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 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.

5. Alunni:
   - Leggono, comprendono ed accettano il documento di E-Safety Policy;
   - Comprendono e rispettano le norme sul diritto d'autore
   - acquisiscono consapevolezza delle situazioni di rischio legate alla rete, telefoni cellulari, fotocamere digitali;
   - Conoscono la politica della scuola sull'uso delle immagini;
   - Capiscono 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.

6. Tecnici informatici:
   - possono controllare ed accedere a tutti i file della intranet;
   - sono gli unici a conoscere la password di rete dell'Istituto;
   - sono gli unici a poter installare nuovi software;
   - limitano attraverso un proxy l'accesso ad alcuni siti;
   - definiscono un account personale per i docenti ed un account di classe in modo da tracciare ogni movimento in rete;
   - la prenotazione dei laboratori avviene attraverso un software della scuola che tiene traccia di ora e laboratorio utilizzati da ciascuno.

7. Direttore dei Servizi Generali e Amministrativi:
   - assicura, nei limiti delle risorse finanziarie disponibili, gli interventi di manutenzione richiesti da cattivo funzionamento e/o danneggiamento della dotazione tecnologica dell'Istituto, controllando al contempo che le norme di sicurezza vengano rispettate;

8. 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 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.

1.3. Condivisione e comunicazione della Policy all'intera comunità scolastica.

Condivisione e comunicazione della Policy ad alunni, personale e genitori attraverso il sito della scuola.
Il dirigente Scolastico regola il comportamento degli studenti ed impone sanzioni disciplinari in caso di comportamento inadeguato

1.4. Gestione delle infrazioni alla Policy.

I provvedimenti disciplinari da adottare da parte del consiglio di classe nei confronti dell'alunno che ha commesso un'infrazione alla policy (in proporzione sia all'età dello studente sia alla gravità dell'infrazione commessa) saranno i seguenti:

- richiamo verbale;
- sanzioni estemporanee commisurate alla gravità della violazione commessa (assegnazione di attività aggiuntive da svolgere a casa su temi di Cittadinanza e Costituzione; divieto temporaneo di prendere parte alla ricreazione e simili);
- 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.

Denunce di bullismo online saranno trattate in conformità con la legge attuale

1.5. Monitoraggio dell'implementazione della Policy e suo aggiornamento.

Il monitoraggio della Policy avrà cadenza annuale a cura del Dirigente scolastico e del referente d'Istituto.
Ogni eventuale aggiornamento avverrà sulla base di casi problematici riscontrati e della loro gestione e sul riscontro di questionari somministrati ad alunni e docenti atti a verificare l'insorgenza di nuove necessità e la revisione di tecnologie esistenti.

1.6. Integrazione della Policy con Regolamenti esistenti.

Il presente documento si integra per obiettivi e contenuti con i seguenti documenti che specificano le politiche dell'Istituto per un uso efficace e consapevole del digitale nella didattica:

- PTOF, incluso il piano per l'attuazione del PNSD;
- Regolamento interno d'istituto;
- Regolamento per l'utilizzo dei laboratori di informatica.

2 Formazione e Curricolo

2.1 Curricolo sulle competenze digitali per gli studenti

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

La scuola si preoccupa pertanto di 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.

2.2 Formazione dei docenti sull'utilizzo e l'integrazione delle TIC nella didattica

Le attività di formazione si svolgeranno su due livelli:

- formazione istituzionale, organizzata dal Miur secondo il PNSD, attraverso gli snodi formativi;
- formazione specifica di Istituto, legata alle esigenza formative rilevate;
- Saper comprendere il potenziale delle tecnologie di networking per costruire una conoscenza collaborativa con altri Paesi (Erasmus+ KA2)

2.3 Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali:

In base a quanto previsto dal Piano Nazionale Scuola Digitale, per soddisfare le richieste di conoscenza e approfondimento delle tecnologie utili alla didattica sono stati previsti alcuni incontri formativi interni alla scuola mentre per promuovere un uso consapevole della rete sono stati attivati corsi a livello di ambito.

2.4 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/)

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

3.1 Accesso ad internet: filtri antivirus e sulla navigazione.

I docenti possono accedere alla rete Wi-Fi della scuola con 2 dispositivi per compilare il registro elettronico o per motivi didattici.

L'Istituto è dotato di 3 laboratori linguistici e altri 4 informatici nei quali la rete è cablata ma segue le stesse politiche di protezione dei dati della rete Wi-Fi

3.2 Gestione accessi (password, backup, ecc.)

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

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

È possibile effettuare installazioni e aggiornamenti di software solo tramite la password di amministratore, fornita al personale di assistenza tecnica.

E' previsto un backup automatico su server esterno.

3.3 E-mail

La scuola è stata registrata sulla piattaforma offerta da Google: Google App for Education pertanto ogni studente e tutto il personale della scuola hanno a disposizione un indirizzo di posta elettronica nome.cognome@iispanzini.com ed uno spazio illimitato cloude per archiviare i condividere materiali su Drive.

3.4 Blog e 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.

3.5 Social network

L'istituto ha una pagina Facebook per la pubblicazione di eventi o attività della scuola ma attualmente i social network non vengono utilizzati nella didattica e l'intranet ne impedisce l'accesso a meno che non ci sia un progetto specifico che ne richieda l'utilizzo.

3.6 Protezione dei dati personali.

L'ufficio tecnico informatico ha pubblicato sul sito scolastico un modulo di implementazione delle misure minime di sicurezza al fine di certificare lo stato di attuazione delle stesse come previsto dalla legislazione vigente.

4 Strumentazione personale

4.1 Per gli studenti: gestione degli strumenti personali - cellulari, tablet ecc..

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

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

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.

4.3 Per il personale della scuola: gestione degli strumenti personali - cellulari, tablet ecc..

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

5 Prevenzione, rilevazione e gestione dei casi

5.1 Prevenzione

- **Rischi**: La prima responsabilità degli insegnanti consiste nell'imparare a riconoscere i rischi più comuni che i ragazzi possono correre sul web, per potere poi intervenire

adeguatamente. Le tipologie di cyberbullismo possono essere catalogate nel modo seguente:

- 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 on line incessante,
- Impersonation: furto di identità,
- Tricky o Outing: il cyberbullo pubblica on line a tuo nome informazioni imbarazzanti .

▪ **Azioni**:

L'obiettivo che l'insegnante deve proporsi dopo avere riconosciuto il pericolo è **non ignorare la richiesta d'aiuto** con 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, vi sono le seguenti:

- diffondere un'informazione capillare rivolta al personale scolastico, agli studenti e alle famiglie, sui rischi che i minori possono correre sul web;
- far rispettare il divieto di utilizzo di dispositivi digitali propri, quali cellulare e smartphone, agli studenti in orario scolastico. Le dovute eccezioni (uso del cellulare per comunicazioni alunno-famiglia in occasione di uscite didattiche o per scopi didattici) andranno espressamente regolamentate e dovranno comunque avvenire sotto 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 (black list).

5.2 Rilevazione

▪ **Che cosa segnalare**

Tra i contenuti andranno opportunamente segnalati:

- dati sensibili o riservati pubblicati in chat o social network (foto, immagini, video personali, informazioni private proprie o 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 riconducibili alla sfera sessuale: messaggi, immagini o video a sfondo sessuale, come foto di nudo o semi-nudo, ecc.

▪ **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 del sotto indicato modello per tenere traccia di tutte le segnalazioni e qualora sia necessario, chiedere supporto alle Associazioni territoriali o alla Polizia Postale.

Segnalazioni situazione di rischi on line o casi di cyberbullismo

N°	Data	Episodio (sintesi)	Azioni intraprese		Insegnante a cui l'alunno si è rivolto	Firma
			Specificare l'azione?	Specificare Chi ha svolto l'azione?		

- **Come gestire le segnalazioni.**

- Raccogliere la segnalazione dell'alunno corredata da prove che attestino l'azione avvenuta;
- Indicare all'alunno a chi può rivolgersi per avere consigli o supporto;
- Sensibilizzare, qualora lo si ritenga utile, la classe in modo che possa essere di supporto psicologico alla vittima;
- Informare tempestivamente le famiglie in merito all'accaduto, anche per consentire ulteriori indagini e, in assenza di prove oggettive, raccogliere testimonianze sui fatti da riferire al Dirigente Scolastico, al referente d'istituto ed, eventualmente, alla Polizia Postale.

5.3 Gestione dei casi

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

  Presa in carico da parte dell'insegnante che può rivolgersi alle seguenti figure:
  - Dirigente scolastico
  - Polizia di stato/ Polizia postale
  - Telefono azzurro (chat anonima o numero verde 19696)
  - Save the children
  - Numero verde **800669696** (Ministero della Pubblica Istruzione: campagna "Smonta il bullo")

  Per i reati più gravi la scuola si rivolgerà direttamente agli organi di Polizia competenti.

Allegati:

- Procedure operative per la gestione delle infrazioni alla Policy
- Tabella per le Segnalazioni dei casi
- Consigli per i genitori

Referente d'Istituto — Dirigente scolastico

(prof.ssa Laura Fagioli) — (prof. Sergio Lombardi)