ISTITUTO COMPRENSIVO STATALE "San Francesco"

Allegato 7 al regolamento generale

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'IC "San Francesco" di Jesi e la rilevazione e gestione delle problematiche connesse a un uso non consapevole delle tecnologie digitali.

Visto anche il progetto www.generazioniconnesse.it , si definiscono qui le misure che l'Istituto intende adottare con le seguenti finalità:

a) promuovere l'educazione all'uso consapevole della rete internet e l'educazione ai diritti e ai doveri legati all'utilizzo delle tecnologie informatiche;

b) prevenire fenomeni legati ai rischi delle tecnologie digitali;

c) segnalare i casi individuati all'interno della scuola;

d) gestire i 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 cyber bullismo che non si configurino come reato, i genitori dei minori coinvolti (o chi ne esercita la responsabilità
   - genitoriale o i tutori)
   - regola il comportamento degli studenti ed impone sanzioni disciplinari in caso di comportamento inadeguato.
2. Referente cyber bullismo d'Istituto:
   - coordina iniziative di prevenzione e contrasto del cyber bullismo 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 cyber bullismo);

- 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;
- 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.

6. Direttore dei Servizi Generali e Amministrativi:

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

7. Genitori:

- contribuiscono, in sinergia con il personale scolastico, alla sensibilizzazione dei propri figli sul tema della sicurezza in rete;
- 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).

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.

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) sono gli stessi previsti nel Regolamento della Scuola Secondaria.

Eventuali denunce di bullismo online saranno trattate in conformità con la normativa vigente.

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;

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 cyber bullismo e le persone e/o associazioni a cui rivolgersi per chiedere consiglio;
- rispettare i copyright.

2.2 Formazione dei docenti sull'utilizzo consapevole delle TIC

Le attività di formazione si svolgeranno su diversi livelli:

- formazione istituzionale, organizzata dal MIUR secondo il PNSD, attraverso gli snodi formativi;
- formazione istituzionale in contrasto al bullismo, organizzata dalla provincia attraverso un progetto di una scuola polo che prevede:
  - interventi su classi individuate dalla scuola stessa,
  - interventi che vedono la presenza dell'intera comunità educante, compresi i genitori,
  - formazione dei referenti di istituto;

2.3 Sensibilizzazione delle famiglie

Il presente documento verrà pubblicato sul sito ed affiancato da incontri mirati (ad es. Polizia Postale) ed iniziative di sensibilizzazione, affinché comprendano i rischi della rete e collaborino proficuamente con il personale della scuola.

Eventuali progetti realizzati dagli allievi verranno pubblicati sul sito della scuola al fine di mettere in evidenza e valorizzare il contributo degli studenti.

Le famiglie saranno invitate a prendere visione e 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 per compilare il registro elettronico o per motivi didattici.

3.2 Gestione accessi (password, backup, ecc.)

Nei computer presenti nei laboratori sono previsti diversi profili di accesso con password relative a docenti e studenti.

È possibile effettuare installazioni e aggiornamenti di software solo tramite il responsabile di laboratorio.

3.3 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 - STRUMENTAZIONE PERSONALE

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

Come indicato nel Regolamento e nel Patto di corresponsabilità, gli alunni, qualora li portino a scuola, si impegnano a tenere spenti i telefoni cellulari durante l'orario scolastico, ivi comprese eventuali attività pomeridiane e durante accoglienza e prescuola.

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

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…

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

5 - PREVENZIONE, RILEVAZIONE E GESTIONE DEI CASI

5.1 Prevenzione

a. 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 cyber bullismo 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 cyber bullo pubblica on line a tuo nome informazioni imbarazzanti su di te;

b. 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;
- dotare i dispositivi della scuola di filtri che impediscano l'accesso a siti web non adatti ai minori (black list).

5.2 Rilevazione

a. Che cosa segnalare

Tra i contenuti andranno opportunamente segnalati:

- dati particolari 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.

b. Come segnalare: quali strumenti e a chi

Docente: deve informare il Dirigente scolastico, il referente d'istituto e le famiglie coinvolte in merito all'accaduto ed, eventualmente, la Polizia Postale.

Referente d'istituto: deve compilare apposito modello per tenere traccia di tutte le segnalazioni e qualora sia necessario, chiedere supporto alle Associazioni territoriali o alla Polizia Postale.

Nel modello (MODELLO PER SEGNALAZIONI DI SITUAZIONI DI RISCHI ON LINE O CASI DI CYBERBULLISMO), vanno indicati l'identificativo dell'alunno, la data, l'episodio in questione con una sintesi dei fatti, il nominativo dell'insegnante a cui l'alunno si è rivolto e le azioni intraprese dallo stesso, la firma.

c. Come gestire le segnalazioni

Raccogliere la segnalazione dell'alunno corredata da prove che attestino l'azione avvenuta.

In ogni caso, sarà opportuna una tempestiva informazione delle famiglie in merito all'accaduto, anche per consentire ulteriori indagini e, in assenza di prove oggettive, di raccogliere testimonianze sui fatti da riferire al Dirigente Scolastico 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)
- 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.