MIUR -UFFICIO SCOLASTICO REGIONALE PER IL LAZIO
LICEO STATALE "NICCOLÒ MACHIAVELLI" – ROMA
LINGUISTICO • SCIENZE UMANE • ECONOMICO-SOCIALE

eSafety Policy

- **Introduzione**

Lo sviluppo e l'integrazione dell'uso delle "tecnologie dell'informazione e della comunicazione" (TIC) nella didattica pone nuove attenzioni dal punto di vista del loro uso sicuro e consapevole.

E' compito dell'intera comunità scolastica, genitori inclusi, garantire che gli studenti siano in grado di utilizzare le tecnologie digitali e che lo facciano in modo appropriato.
In questo quadro si inserisce la necessità di dotare la scuola di una propria *Policy di E-safety*, nell'ottica della promozione dell'uso consapevole delle tecnologie digitali e della gestione delle infrazioni attraverso il monitoraggio continuo della *Policy* e la sua integrazione con il *Regolamento d'Istituto.*
Obiettivo del presente documento è quello di educare e sensibilizzare l'intera comunità scolastica all'uso sicuro e consapevole di INTERNET in conformità con le "Linee di orientamento per azioni di prevenzione e di contrasto al bullismo e cyberbullismo" elaborate dal Ministero dell'Istruzione e della Ricerca in collaborazione con il *Safer Internet Center* per l'Italia, programma istituito dalla Comunità Europea.

- **Rapporto tra competenze sociali e civiche e competenze digitali**

La capacità di partecipare in modo costruttivo e consapevole alle comunità *on line* e ai network virtuali costituisce un prerequisito fondamentale per partecipare in modo attivo alla società della conoscenza e dell'informazione. Alla diffusione dei nuovi *media* e degli strumenti del web 2.0 si accompagna infatti l'emergere di nuove opportunità di partecipazione civica e sociale (*e-engagement*, *e-inclusion*), che richiedono capacità comunicative e socio-relazionali adeguate. E' fondamentale quindi conoscere come ci si comporta in queste comunità, quali regole vanno rispettate e quali ruoli e responsabilità hanno i soggetti che vi partecipano.

La scuola, nel farsi carico della formazione globale dell'individuo nella fase evolutiva, deve individuare in maniera chiara e inequivocabile ruoli e responsabilità di ciascuno degli attori del percorso formativo.

Al Liceo "Niccolò Machiavelli" di Roma è in corso un processo di riflessione sulla presenza delle tecnologie dell'informazione e della comunicazione all'interno dell'Istituto. Supportato dalla formazione PNSD a cui ha avuto accesso, il gruppo di lavoro, formato dall'Animatore Digitale e dal Team per l'Innovazione, ha elaborato le seguenti linee guida, di fatto già in buona parte seguite da docenti e studenti.

E' naturalmente un work in progress che prevede aggiornamenti e integrazioni all'interno di una riflessione condivisa da parte di tutte le componenti della scuola.

1. Elementi generali dell'E-Safety Policy

L'E-Safety Policy presenta le linee guida dell'Istituto riguardo all'utilizzo delle tecnologie dell'informazione, che costituiscono parte integrante dell'attività didattica e vengono utilizzate nella comunicazione bidirezionale scuola/ famiglia

1 A. Ruoli e Responsabilità

Il Dirigente Scolastico è responsabile per la sicurezza dei dati ed è garante dell'applicazione delle linee guida contenute nella E-Safety Policy.

L'Animatore Digitale, il Team per l'Innovazione, il Team digitale, il Referente per il Bullismo e il Cyberbullismo aggiornano la policy sul sito della scuola e promuovono la diffusione dei suoi contenuti.

I docenti inseriscono tematiche legate alla sicurezza online nella didattica e guidano gli studenti nelle attività che prevedono l'accesso alla rete.

I genitori sostengono la scuola nel promuovere la sicurezza online,

conoscendo e condividendo la policy e proponendo riflessioni e suggerimenti.

Gli studenti conoscono e rispettano l'E-Safety Policy e segnalano al docente di classe eventuali usi impropri della rete e dei dispositivi.

Il personale non docente conosce l'E-Safety Policy e contribuisce alla sorveglianza.

1 B. Condivisione e comunicazione della E-Safety Policy all'intera comunità scolastica

La E-Safety Policy è pubblicata nella sezione PNSD del sito di Istituto. Essa viene illustrata ai genitori e agli studenti in ogni occasione appropriata (Riunioni degli Organi Collegiali, Open Days, riunioni scuola-famiglie, eventi).

1 C. Gestione delle infrazioni alla E-Safety Policy

Nel caso di infrazioni alle indicazioni della E-Safety Policy che rientrino nella casistica del Punto 3 "Violazione del dovere del rispetto della persona" del "Quadro riassuntivo delle Sanzioni disciplinari" del Regolamento di Istituto, si procede come ivi indicato. In ogni caso va informato il coordinatore di classe, il quale a sua volta riferisce al Dirigente Scolastico e alla famiglia.

1 D. Monitoraggio dell'implementazione della E-Safety Policy e suo aggiornamento

Il Dirigente Scolastico è responsabile dell'implementazione della E-Safety Policy all'interno dell'Istituto. L'Animatore Digitale, il Team per l'Innovazione, il Team digitale, il Referente per il Bullismo e il Cyberbullismo, collaborano con il Dirigente Scolastico, per la revisione e l'aggiornamento del documento.

1 E. I ntegrazione della E-Safety Policy con Regolamenti esistenti

L'E-Safety Policy è coerente con quanto stabilito da:

- Legge 31 dicembre 1996 n. 675 "Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali");
- Statuto delle studentesse e degli studenti della scuola secondaria DPR 24 giugno 1998 n. 249 modificato dal DPR 21 novembre 2007 n. 235;
- Legge 29 maggio 2017 n. 71 "Disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del cyberbullismo";

- Regolamento di Istituto (in particolare artt. 5 bis, 27 quater, 29, 30 e Quadro riassuntivo delle Sanzioni disciplinari punto 3);
- Patto di Corresponsabilità.

2. Formazione e Curricolo

L'impiego corretto e consapevole delle TIC costituisce un fattore di innovazione della didattica e può utilmente contribuire all'aumento della motivazione e del rendimento degli studenti e alla modifica delle pratiche tradizionali di insegnamento: è quindi importante coglierne le potenzialità rispetto a contesti e finalità specifici.
Per sostenere questo processo all'interno della scuola è necessario investire sulla formazione e l'aggiornamento degli insegnanti, soprattutto in relazione alla didattica per competenze e all'innovazione metodologico-didattica.

2 A. Curricolo sulle competenze digitali per gli studenti

Le competenze digitali rientrano tra le 8 competenze chiave di cittadinanza (Raccomandazione del Parlamento Europeo e del Consiglio del 18 dicembre 2006) e, come tali, vengono promosse trasversalmente da tutti i docenti.

Al termine del primo biennio 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

2 B. Formazione dei docenti alle nuove tecnologie applicate alla didattica.

L'Animatore digitale, il Team per l'Innovazione e il Team digitale formulano proposte per il Piano di Formazione Triennale partendo dai bisogni formativi dei docenti in relazione alle nuove tecnologie applicate alla didattica.
Viene data diffusione ai corsi sulle nuove tecnologie applicate alla didattica organizzati dalla Scuola Polo di Ambito, dalle Reti di scuole a cui appartiene l'Istituto, e da enti certificatori (ad esempio formazione eTwinning).

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

L'infrastruttura e la strumentazione TIC dell'Istituto sono un patrimonio di tutti e vanno utilizzate nel rispetto delle norme contenute nel Regolamento d'Istituto e nei Regolamenti dei singoli laboratori multimediali. I danni causati alle attrezzature saranno a carico di chiunque disattenda i suddetti Regolamenti. La scuola deve considerare l'ambiente *on line* alla stregua dell'ambiente fisico e valutarne tutti gli aspetti legati alla sicurezza.
Per quanto concerne l'*hardware* la scuola provvede a pianificare interventi periodici di manutenzione.

3 A. Accesso ad internet

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

3 B. Gestione accessi

La connessione alla rete wireless è riservata ai docenti per fini didattici ed è accessibile tramite password modificata periodicamente.

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.

3 C. Sito web di Istituto

Il sito dil Istituto è raggiungibile all'indirizzo www.ismachiavelli.eu.

Il Dirigente, il Referente del sito ed eventuali altri amministratori in organigramma verificano e aggiornano i contenuti destinati alla pubblicazione.

3 D. Social network

In diverse classi è diffuso l'utilizzo delle piattaforme didattiche Edmodo, eTwinning, AVE, e di Google Drive, sotto la supervisione dei docenti.

La scuola promuove e realizza progetti di educazione all'uso consapevole dei social network in collaborazione con partner esterni qualificati.

3 E. Protezione dei dati personali

In fase di iscrizione degli studenti alla scuola i genitori sottoscrivono l'informativa sul trattamento dei dati personali in ottemperanza all'art. 13 D.Lgs 30 giugno 2003 , n. 196 (Codice in materia di protezione dei dati personali) e rilasciano il consenso all'utilizzo e all'esposizione di materiale fotografico e audiovisivo e di elaborati, anche multimediali, degli studenti, anche in sedi diverse da quelle dell'Istituto (ad esempio pubblicazioni in formato digitale e siti web).

In caso di utilizzo di piattaforme digitali condivise o di strumenti per la creazione e la gestione di classi virtuali viene acquisito preventivamente il consenso informato dei genitori.

In caso di attività di ampliamento dell'offerta formativa, organizzate in collaborazione con Enti esterni, viene richiesto preventivamente ai genitori il consenso informato alle riprese audio e video e al loro eventuale utilizzo per scopi didattici, informativi e divulgativi anche tramite pubblicazione su siti web.

L'accesso ai dati riportati nel registro elettronico è riservato ai genitori tramite l'invio di una password strettamente personale.

4. Dispositivi personali e regole per il BYOD

4 A. Accesso a dispositivi personali

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 dispostivi elettronici personali per scopi didattici (modalità BYOD, Bring your own device).

Per i docenti: durante l'orario di servizio l'utilizzo di dispostivi 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.

4 B. Regole per il BYOD

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 rivelarli 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.

5. Prevenzione

Prevenzione

La scuola si impegna ad attrezzare le aule con dispositivi elettronici sicuri e protetti.

I docenti si impegnano ad organizzare e condividere con gli studenti momenti di riflessione sull'utilizzo consapevole di internet e degli strumenti tecnologici e a formarsi su queste tematiche.

I genitori si impegnano a prendere visione della E-safety Policy e a seguire e sostenere le azioni promosse dalla scuola per l'utilizzo consapevole della rete.

Gli studenti si impegnano a rispettare i regolamenti e a partecipare attivamente alle occasioni di confronto sulle tematiche dell'utilizzo consapevole delle TIC promosse e organizzate dalla scuola.

Per i rischi connessi all'utilizzo delle nuove tecnologie (adescamento online, cyberbullismo, furto di identità, sexting), la scuola organizza incontri informativi e formativi per docenti, studenti e genitori, avvalendosi anche di consulenti esterni.

Roma, 8.1.2018

Il Dirigente Scolastico

(Prof.ssa Elena Zacchilli)

L'Animatore Digitale

(Prof.ssa Maria Rosaria Fasanelli)

Il Referente per il bullismo e il cyberbullismo

(Prof.ssa Vittoria Antonucci)

Il Team per L'Innovazione

(Prof.ssa Barbara Antonini)

(Prof.ssa Vittoria Antonucci)

(Prof.ssa Gabriella Pastore)