ISTITUTO COMPRENSIVO DI CANDIOLO
P.le DELLA RESISTENZA, SNC - 10060 CANDIOLO (TO
TEL: 011/9622308-309-FAX:011/9622792
E-MAIL : toic83400e@istruzione.it – toic83400e@pec.istruzione.it – www.iccandiolo.gov.it
C.F. 94043140014 – Codice Univoco Ufficio. UFQOJT

E-SAFETY POLICY

Rev. 01 del 26/11/2018

GRUPPO DI LAVORO:

Agostini Graziana
Battaglia Ursula
Caprio Pietro
Di Cesare Valeria
Eblovi Anna Maria
Giacosa Gabriella
Giraud Jessica
Golzio Donata
Menegon Irene
Smeriglio Franca
Ressia Barbara
Rosso Liliana

INDICE DEI CONTENUTI

1. INTRODUZIONE

1.1 **Scopo della *policy*.**

Lo scopo della E-Safety Policy è:

- salvaguardare e proteggere i bambini, i ragazzi e lo staff dell'Istituto;
- assistere il personale della scuola a lavorare in modo sicuro e responsabile con le tecnologie digitali;
- impostare chiare procedure di comportamento e/o codici di condotta rilevanti per un uso responsabile di Internet a scopo didattico, personale;
- indicare le azioni per affrontare gli abusi online come il cyberbullismo;
- garantire che tutti i membri della comunità scolastica (allievi, docenti, personale ATA, genitori) siano consapevoli che, a fronte di un comportamento illecito o pericoloso, saranno intraprese le opportune azioni disciplinari e giudiziarie;
- sensibilizzare i docenti e tutto il personale scolastico sull'importanza della formazione nell'ambito delle nuove tecnologie;
- sensibilizzare i docenti sull'importanza di costruire un curricolo trasversale per l'acquisizione delle competenze digitali in ogni ordine di scuola.

Le principali aree di rischio nella rete per la nostra comunità scolastica possono essere riassunte come segue:

<u>Contenuti</u>

- esposizione involontaria a contenuti inappropriati (a causa ad es. di intromissioni tramite maleware, foto condivise da altri su social network)
- visita di siti web inappropriati
- visita di siti di odio
- informazioni online non corrette o non autentiche.

<u>Contatti attraverso social network</u>

- grooming
- sexting
- bullismo online in tutte le forme
- furto di identità
- opinioni, insulti in anonimato

<u>Comportamenti</u>

- divulgazione di informazioni e immagini personali o altrui (privacy)
- reputazione online
- salute e benessere (quantità di tempo speso online su Internet o giochi)
- sexting (invio e ricezione di immagini personali intime)
- partecipazione a chat in forma anonima
- estremismo
- copyright (poca cura o considerazione per i diritti d'autore relativamente a musica e film).

1.2 **Ruoli e responsabilità**

Dirigente scolastico è

- responsabile generale per i dati e la sicurezza dei dati;
- garante di un utilizzo di un Internet Service filtrato, approvato e conforme ai requisiti delle leggi vigenti;
- responsabile di assicurare che il personale riceva una formazione adeguata per svolgere i ruoli di sicurezza online e per aggiornare altri colleghi;
- consapevole delle procedure da seguire in caso di infrazione della E–Safety Policy;
- destinatario delle relazioni di monitoraggio periodiche sulla sicurezza online da parte dell'Amministrazione di Sistema;
- coordinatore delle azioni da intraprendere con le autorità locali e le agenzie competenti, in caso di infrazioni.

Amministrazione di Sistema (la figura può essere ricoperta da un tecnico competente esterno) ha la funzione di:

- evidenziare i problemi di sicurezza online;
- redigere e diffondere procedure per la sicurezza informatica;
- garantire che sia tenuto un registro di incidenti di sicurezza online;
- controllare l'accesso a materiali illegali/inadeguati.

Funzione strumentale ambienti digitali / Animatore digitale e Team digitale si occupano di:

- promuovere la consapevolezza e l'impegno per la salvaguardia online in tutta la comunità scolastica;
- sensibilizzare tutto il corpo docente affinché l'educazione alla sicurezza online sia incorporata in tutto il programma di studi;
- facilitare la formazione e la consulenza per tutto il personale della scuola;
- pubblicare la E-Safety Policy sul sito della scuola;
- diffondere la E- Safety Policy a tutta la comunità scolastica;
- garantire che tutti i dati pubblicati sul sito, relativi agli alunni, siano sufficientemente tutelati;
- rivedere ed eventualmente aggiornare annualmente il documento di E-Policy.

Responsabile per il cyberbullismo e Commissione Rete SHE si occupano di:

- promuovere iniziative volte a migliorare le relazioni tra gli allievi (tolleranza, rispetto del diverso ...) in tutti gli ordini di scuola;
- promuovere iniziative rivolte a tutta la comunità scolastica e mirate a riconoscere e contrastare il cyberbullismo;
- rendere consapevoli i docenti e tutto il personale scolastico della normativa vigente in tema di cyberbullismo;
- monitorare e controllare possibili azioni di cyberbullismo.

Il personale docente ha il compito di:

- favorire l'utilizzo delle TIC nella didattica;
- inserire, in tutti gli aspetti del programma di studi e di altre attività scolastiche, tematiche legate alla sicurezza online;
- supervisionare e guidare gli alunni quando sono impegnati in attività di apprendimento che coinvolgono la tecnologia online;
- favorire l'uso consapevole del web per effettuare ricerche online;
- sensibilizzare gli alunni sui problemi legali relativi all'uso scorretto di contenuti elettronici, come ad esempio le leggi sul copyright;
- educare gli allievi al rispetto dell'E-Policy, in ogni ordine scolastico e a seconda dell'età;
- favorire progetti finalizzati al rispetto e alla tolleranza reciproca.

Il personale ATA ha il compito di:

- leggere e rispettare la presente E-Policy;
- avere consapevolezza circa le questioni di sicurezza informatica dell'Istituto;
- segnalare qualsiasi abuso sospetto o problema ai responsabili della sicurezza online.

Gli alunni devono:

- rispettare l'E-Policy in ogni ordine scolastico, a seconda dell'età;
- utilizzare in maniera consapevole il web per effettuare ricerche online;
- rispettare le normative sul diritto d'autore;
- capire l'importanza di segnalare abusi, l'uso improprio e l'accesso a materiali inappropriati;
- sapere quali azioni intraprendere se loro, o qualcuno che conoscono, si sente preoccupato o vulnerabile quando si utilizza la tecnologia online;
- conoscere e capire la politica della scuola relativa all'uso dei telefoni cellulari, fotocamere digitali e dispositivi portatili e alla diffusione responsabile delle immagini;
- capire l'importanza di adottare buone pratiche di sicurezza online quando si usano le tecnologie digitali fuori dalla scuola;
- assumersi la responsabilità di conoscere i benefici e i rischi di utilizzo di Internet e delle altre tecnologie in modo sicuro, sia a scuola che a casa.

I genitori hanno il compito di:

- sostenere la scuola nel promuovere la sicurezza online e condividere l'accordo di l'E-Policy con la scuola;
- accedere al sito web della scuola in conformità con quanto stabilito dalla stessa;
- conoscere e capire la politica della scuola relativa all'uso dei telefoni cellulari, fotocamere digitali e dispositivi portatili e alla diffusione responsabile delle immagini;
- guidare i propri figli a capire l'importanza di adottare buone pratiche di sicurezza online quando si usano le tecnologie digitali fuori dalla scuola;
- assumersi la responsabilità di conoscere i benefici e i rischi di utilizzo di Internet e delle altre tecnologie in modo sicuro a casa;
- essere consapevoli dei rischi legati alla divulgazione sui social di informazioni relative alla scuola.

1.3 **Condivisione e comunicazione dell'E-Policy**

Per evitare che l'adozione di questa l'E-Policy rappresenti solo un atto formale, l'Istituto si impegna a prendere spunto da essa come base di partenza per una serie di azioni e iniziative:

- pubblicazione sul sito della scuola;
- attivazione di momenti informativi e di discussione e condivisione dei contenuti, ad esempio:
  - per il corpo docente, discussione collegiale sui contenuti;
  - per la componente studentesca, discussione in classe della E-Policy;
  - per i genitori, organizzazione di incontri di sensibilizzazione sul tema della sicurezza informatica.

1.4 **Gestione delle infrazioni**

Le infrazioni alla E-policy possono essere rilevate da docenti/ATA nell'esercizio delle proprie funzioni oppure possono essere segnalate da alunni e genitori a docenti/ATA.
Qualora esse si configurino come vero e proprio reato, occorre darne tempestiva segnalazione al Dirigente Scolastico per gli adempimenti del caso.
Infatti è bene ricordare a tutti che nel momento in cui un qualunque attore della comunità scolastica venga a conoscenza di un reato perseguibile d'ufficio, è fatto obbligo di denuncia (ex art. 331 del codice di procedura penale). L'omissione di denuncia costituisce reato (art. 361).
Nel caso in cui le infrazioni della E-policy violino norme previste dal Regolamento di Istituto si procede secondo quanto previsto dal Regolamento stesso; qualora le infrazioni riguardino l'opportunità di certi comportamenti o la convivenza civile, la scuola eroga delle sanzioni secondo il principio della sensibilizzazione in uno spirito di recupero e rieducazione.

1.5 **Integrazione della E-Policy con i Regolamenti esistenti**

La presente E-Policy viene allegata al PTOF

2. FORMAZIONE E CURRICOLO

2.1 **Curricolo sulle competenze digitali per la componente studentesca**

Il corpo docente dell'I.C. Candiolo si attiva per far perseguire agli alunni le competenze digitali previste dal curricolo di tale disciplina, dalle Nuove Indicazioni e in linea con quanto atteso dai progetti innovativi presenti nel PTOF, per ogni classe dalla Scuola dell'Infanzia alla Scuola Secondaria di 1 ^{0} grado.

2.2 **Formazione del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica; formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.**

La formazione del corpo docente verrà organizzata su due livelli: interno ed esterno.
A livello interno si prevede che una parte della formazione in servizio obbligatoria ai sensi della L. 107/2015 sia dedicata proprio all'uso e all'inserimento delle TIC nella didattica e ai temi informatici in generale.
Tale formazione può essere svolta da docenti dell'Istituto che hanno seguito corsi specifici, in particolare dai docenti che fanno parte del Team digitale, per cui il MIUR prevede opportuni percorsi la cui ricaduta viene annualmente adattata alle esigenze dell'Istituto da parte del Collegio Docenti, ed è improntata alla condivisione di esperienze significative e di buone pratiche.
Per quanto riguarda la formazione esterna, la scuola assicura attraverso la diffusione nell'area riservata del sito scolastico, tempestiva e capillare informazione su corsi, convegni e seminari che riguardino tali argomenti, cercando altresì di agevolare il personale che intenda parteciparvi. Infine la scuola può aderire a progetti appositi di formazione presentati da enti e associazioni.

3. GESTIONE DELL'INFRASTRUTTURA E DELLA STRUMENTAZIONE TIC DELLA SCUOLA

3.1 Accesso ad Internet

Configurazione del software di navigazione con limitazione a siti proibiti e installazione di filtri di sicurezza.

3.2 Gestione accessi

I computer docenti devono essere protetti da password di accesso e sospensione attività.
I computer degli alunni hanno accesso libero non protetto da password.
Tutti i computer di ultima generazione hanno doppio account (amministratore/utente).
L'accesso alla rete WIFI è coperto da password e l'utilizzo è riservato al personale scolastico per motivi di studio o lavoro.

3.3 E-mail

L'Istituto fornisce attualmente una casella di posta elettronica @iccandiolo.gov.it ai responsabili di plesso e all'amministratore del sito web.
Sulla rete scolastica tutti sono invitati a utilizzare solo l'account di posta elettronica @istruzione.it e @iccandiolo.gov.it, se in possesso, e per scopi inerenti lo svolgimento didattico/organizzativo.
Le comunicazioni tra personale scolastico, famiglie e allieve/allievi via e-mail devono avvenire preferibilmente tramite un indirizzo e-mail @iccandiolo.gov,it o @istruzione.it, per consentire l'attivazione di protocolli di controllo.
In alternativa alla mail le comunicazioni possono avvenire attraverso la piattaforma didattica (es. Edmodo) o tramite registro elettronico quando accessibile per le famiglie.
Le comunicazioni al personale scolastico delle pubblicazioni periodiche sul sito vengono gestite attraverso mail provenienti dall'amministratore del sito web.
E-mail in arrivo da mittenti sconosciuti vanno trattate come sospette ed eventuali allegati non devono essere aperti.

3.4 Sito web della scuola.

É gestito dalla Funzione Strumentale preposta che pubblicherà documentazione e informazioni inerenti alla scuola.
Le foto e i video di attività didattiche afferenti ad attività istituzionali della scuola inserite nel PTOF saranno pubblicate sul sito previo consenso dei genitori o tutori rispettando le disposizioni legislative vigenti in merito.
Il sito prevede un'area pubblica per le informazioni che non comportano la diffusione di dati personali o riservati, in cui sono reperibili le informazioni sulla vita scolastica, iniziative, corsi, scadenze ministeriali, avvisi di carattere generale e un'area riservata accessibile solo dopo autenticazione da parte del personale scolastico.
Il personale che è in possesso delle credenziali per la gestione dei contenuti sul portale si assumerà la responsabilità editoriale di garantire che il contenuto inserito sia accurato e appropriato.

3.5 Social network.

L'utilizzo dei social network nella scuola è consentito solo ed esclusivamente per finalità didattiche, lavorative e/o di studio. Nella pratica didattica si devono utilizzare piattaforme social dedicate al mondo scolastico al fine di garantirne la sicurezza (es. Edmodo). Inoltre si cerca di educare la componente studentesca all'uso sicuro dei social network in generale. Gli alunni non devono pubblicare senza permesso foto personali proprie o altrui su qualsiasi spazio di social network previsto nella piattaforma di apprendimento scolastico. Alunne/alunni, genitori e personale docente/ATA saranno informati sull'uso sicuro degli spazi di social network e sulle conseguenze legali di ogni uso improprio.

3.6 Protezione dei dati personali.

I dati personali saranno trattati esclusivamente dal personale della scuola incaricato, secondo la normativa vigente.
Vengono individuate a seguire alcune linee guida:
- le fotografie o i video da pubblicare sul sito che includano allieve e allievi saranno selezionati con cura e non permetteranno a singoli di essere chiaramente identificati a meno che non si tratti di eventi particolari per cui le famiglie potranno fornire opportuna autorizzazione. La scuola cercherà di utilizzare fotografie o video di gruppo piuttosto che foto integrali di singoli;
- nomi completi di alunne e alunni saranno evitati sul sito web, in particolare se in associazione con le loro fotografie;
- ogni evento sarà preso in considerazione per stabilire l'opportunità di pubblicare dati personali e sarà presentata apposita richiesta circostanziata.

4. STRUMENTAZIONE PERSONALE

4.1 Per la componente studentesca

Come previsto nel PNSD si intende sperimentare il BYOD, per cui gli alunni potranno portare a scuola i propri dispositivi digitali ed utilizzarli per le attività didattiche avendo anche accesso alla Rete nel rispetto delle regole stabilite dalla scuola.
Agli studenti è vietato l'utilizzo di telefoni cellulari in orario scolastico, se non su indicazione dei docenti.
E' possibile adoperare pen drive, CD o DVD solo previa autorizzazione dell'insegnante e dopo aver effettuato un apposito controllo con antivirus.

4.2 Per il personale docente/ATA.

Tutto il personale scolastico è tenuto ad ottemperare alla normativa vigente che impedisce l'uso del cellulare a scuola tranne in situazioni di emergenza e a fini didattici.
Il personale preferirà, quando ciò è possibile, l'impiego della strumentazione fornita dalla scuola rispetto a quella personale (portatili, pc fissi, …); le infrastrutture e gli apparati della scuola non vanno utilizzati per scopi personali. Telefoni cellulari, tablet, fotocamere e altri strumenti di registrazione audio/video non devono essere impiegati durante le lezioni scolastiche se non all'interno di attività didattiche espressamente programmate.
La password di accesso alla rete WIFI va custodita con cura e per nessuna ragione deve essere divulgata a chi non ha titolo per utilizzarla.
Qualora si utilizzino a scuola dispositivi di archiviazione esterna di proprietà personale (CD, DVD, pen drive, dischi fissi portatili) è bene controllare preventivamente che essi siano esenti da virus per evitare di danneggiare le attrezzature comuni.

5. PREVENZIONE, RILEVAZIONE E GESTIONE DEI CASI[1]

Le misure di prevenzione comprendono l'integrazione nel curricolo dei temi legati al corretto utilizzo delle TIC e di Internet: la progettazione di unità didattiche specifiche deve essere pianificata a livello di dipartimenti disciplinari, garantendo un intervento su ogni classe, anche con docenti non titolari della classe. Si demanda ai settori disciplinari la scelta dei settori su cui focalizzare la formazione: a titolo di esempio il dipartimento letterario si può soffermare in particolare sugli aspetti legati all'affettività, alla socializzazione e alla cittadinanza, quello tecnologico-scientifico-matematico sulle questioni tecniche e legate alla salute, quello di arte/musica sulla tutela del diritto d'autore, …
La scuola si avvale della collaborazione di enti e associazioni per realizzare incontri rivolti alla componente studentesca e alle famiglie con l'intento di fornire ogni elemento utile alla prevenzione e alla gestione dei problemi relativi alla sicurezza informatica; le famiglie sono invitate a proporre tematiche di particolare interesse su cui la scuola focalizzerà il proprio intervento.
Il Collegio Docenti più volte si è espresso favorevolmente per l'attivazione di uno sportello di ascolto al quale gli alunni si può rivolgere per avere consigli e sostegno psicologico anche relativamente alle tematiche del cyberbullismo.
La rilevazione dei casi è compito dell'intera comunità educante, secondo la sensibilità di ciascuno e la presenza in particolari momenti o contesti. A partire dalla corretta formazione e sensibilizzazione di tutti gli adulti coinvolti, tutto il personale scolastico è invitato ad essere attento a ciò che le ragazze

[1] Tratto e rielaborato dal documento di E-Safety Policy dell'Istituto Umberto Saba di Torino

e i ragazzi vivono evitando ogni atteggiamento accusatorio o intimidatorio per riuscire a ricevere dai minori più fragili segnalazioni e confidenze circa situazioni problematiche vissute.
Le/gli insegnanti potranno così accorgersi tempestivamente di quanto accade e compiere azioni immediate di contrasto verso gli atti inopportuni, seppur non illegali, per poter evitare conseguenze a lungo termine che possano pregiudicare il benessere e una crescita armoniosa dei soggetti coinvolti.
La gestione dei casi rilevati va differenziata a seconda della loro gravità; fermo restando che è necessaria la condivisione a livello di Team/Consiglio di Classe di ogni episodio anche minimo: alcuni avvenimenti possono essere affrontati e risolti con la discussione collettiva in classe, altri possono essere affrontati convocando genitori e alunno/a per riflettere insieme su quanto accaduto e come rimediare. Nei casi più gravi e in ogni ipotesi di reato occorre valutare tempestivamente con il Dirigente Scolastico come intervenire.

PREVENZIONE, RILEVAZIONE E GESTIONE

RISCHI	AZIONI
Adescamento online (grooming)	Sensibilizzazione sull'esistenza di individui che usano la rete per instaurare relazioni, virtuali o reali, con minorenni e per indurli alla prostituzione. Qualora si venga a conoscenza di casi simili, occorre valutarne la fondatezza e avvisare il Dirigente Scolastico per l'intervento delle forze dell'ordine.
Cyberbullismo	Campagne di sensibilizzazione e informazione anche con l'ausilio di progetti e realtà esterni. I casi possono essere molto variegati, variando dal semplice scherzo di cattivo gusto via social (anche in anonimato) a vere e proprie minacce verbali e fisiche, che costituiscono reato. Occorre confrontarsi con il Dirigente Scolastico sulle azioni da intraprendere.
Dipendenza da Internet, videogiochi, shopping o gambling online, ...	Informazioni sul fatto che ciò può rappresentare una vera e propria patologia che compromette la salute e le relazioni sociali e che in taluni casi (per es. uso della carta di credito a insaputa di altri) rappresenta un vero e proprio illecito.
Esposizione a contenuti pornografici, violenti, razzisti, ...	Verso i genitori: informazione circa le possibilità di attivare forme di controllo parentale della navigazione e sensibilizzazione sulla necessità di monitorare l'esperienza online dei propri figli. Verso la componente studentesca: inserimento nel curricolo di temi legati all'interculturalità, al rispetto delle diversità e alla affidabilità delle fonti online. Qualora si venga a conoscenza di casi simili, occorre convocare i genitori per richiamarli a un maggiore controllo sulla fruizione di Internet da parte dei propri figli e/o sulla necessità di non usufruirne in presenza degli stessi.
Sexting e pedopornografia.	Verso i genitori: informazione circa le possibilità di attivare forme di controllo parentale della navigazione. Verso la componente studentesca: inserimento nel curricolo di temi legati all'affettività, alla sessualità, al rispetto delle differenze. In casi simili, se l'entità è lieve occorre in primo luogo parlarne con alunne e alunni e rispettivi genitori, ricordando loro che l'invio e la detenzione di foto che ritraggono minorenni in pose sessualmente esplicite configura il reato di distribuzione di materiale pedopornografico. I 'nativi digitali' spesso non sono consapevoli che una foto o un video diffusi in rete potrebbero non essere tolti mai più né sono consapevoli di scambiare o diffondere materiale pedopornografico. In casi di rilevante gravità occorre informare tempestivamente il Dirigente Scolastico per gli adempimenti del caso.
Violazione della privacy	Informazione sull'esistenza di leggi in materia di tutela dei dati personali e di organismi per farle rispettare. Se il comportamento rilevato viola solo le norme di buona convivenza civile e di opportunità, occorre convocare i soggetti interessati per informarli e discutere dell'accaduto e concordare forme costruttive ed educative di riparazione. Qualora il comportamento rappresenti un vero e proprio illecito, il Dirigente Scolastico deve esserne informato in quanto, a seconda dell'illecito, sono previste sanzioni amministrative o penali.

Candiolo, 20/11/2018

La commissione

Il Dirigente scolastico
Claudia Torta