



I.C. "CAIO GIULIO CESARE" - OSIMO

DOCUMENTO E-SAFETY POLICY **(Approvato a settembre 2018)** **a.s. 2017/2018** **2018/2019**

1. Introduzione

- Scopo della policy
- Ruoli e responsabilità
- Condivisione e comunicazione della Policy all'intera comunità scolastica
- Gestione delle infrazioni della policy
- Monitoraggio e aggiornamento della policy
- Integrazione della policy con regolamenti esistenti

2. Formazione e curriculum

- Curriculum sulle competenze digitali per gli studenti
- Formazione dei docenti sull'utilizzo e l'integrazione delle TIC nella didattica
- Formazione dei docenti sull'utilizzo consapevole e sicuro di internet delle tecnologie digitali
- Sensibilizzazione delle famiglie

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

- Accesso a internet
- Blog e sito web della scuola
- Social network
- Protezione dei dati personali

4. Strumentazione personale

- Per i docenti e il personale della scuola: gestione degli strumenti personali
- Per gli studenti: gestione degli strumenti personali

5. Prevenzione, rilevazione e gestione dei casi

- Prevenzione (rischi e azioni)

- Rilevazione
- Gestione dei casi

1. INTRODUZIONE

Lo scopo della E-Safety Policy è di promuovere l'uso consapevole e critico delle tecnologie digitali e di Internet, seguendo le indicazioni di **Educazione Civica Digitale** emanate dal Miur, per salvaguardare e proteggere gli studenti e tutto il personale dell'Istituto; assistere il personale della scuola a lavorare in modo sicuro e responsabile; impostare chiare aspettative di comportamento e/o codici di condotta rilevanti per un uso responsabile di Internet a scopo didattico, personale o ricreativo; affrontare gli abusi online come il cyberbullismo; garantire che tutti i membri della comunità scolastica siano consapevoli del fatto che il comportamento illecito o pericoloso è inaccettabile e che saranno intraprese le opportune azioni disciplinari e giudiziarie.

Tenendo conto del piano d'azione elaborato, della sua complessità e della quantità delle azioni definite e da realizzare, il piano stesso verrà realizzato in un triennio.

Il documento potrà essere implementato e revisionato annualmente.

Scopo della policy

- visione del fenomeno
- norme comportamentali e procedure per l'utilizzo delle TIC a scuola
- misure per la prevenzione e la rilevazione e gestione delle problematiche connesse ad un uso non consapevole delle tecnologie digitali.

L'Istituto ha l'obiettivo di promuovere le competenze di cittadinanza digitale sensibilizzando docenti, studenti e famiglie relativamente all'uso consapevole di Internet e delle tecnologie digitali.

I docenti hanno il compito di responsabilizzare gli studenti nell'uso consapevole e responsabile delle apparecchiature della scuola, che sono patrimonio comune, e nel seguire le corrette norme di utilizzo.

Per garantire la sicurezza in rete la scuola ha previsto le seguenti strategie:

- promuovere la partecipazione dei docenti a corsi di formazione sull'uso delle TIC nella didattica e sull'uso consapevole di Internet;
- condividere materiali (guide, manuali, ecc..) sull'uso consapevole di Internet e delle tecnologie digitali;
- organizzare incontri per docenti, alunni, genitori dedicati alla prevenzione dei rischi associati all'uso di Internet delle tecnologie digitali;
- dotare di firewall per la navigazione in internet;
- controllo periodico del sistema informatico;
- accesso con password nei computer scolastici.

La presente policy si applica a tutti i componenti della comunità scolastica che hanno accesso al sistema informatico della scuola o sono utenti dello stesso.

Ruoli e responsabilità

Ogni utente connesso alla rete deve:

- rispettare il presente regolamento e la normativa vigente;
- tutelare la propria privacy, quella degli altri adulti e quella degli studenti;
- rispettare la "netiquette", galateo della rete.

Netiquette

- a. rispettare le altre persone, non sono permessi discriminazione e razzismo;
- b. essere tolleranti con chi ha poca dimestichezza con le TIC;
- c. non rivelare dettagli o informazioni, come indirizzo o numero di telefono, proprie o di altre persone;
- d. ottenere sempre il permesso prima di iscriversi a mailing-list o siti web che lo chiedono;
- e. non fornire indirizzo e numero di telefono a persone incontrate sul web senza chiedere il permesso ai genitori o ai docenti;
- f. non inviare fotografie proprie o di altre persone;
- g. chiedere il permesso prima di scaricare materiale dal web di vario tipo;

RUOLO	RESPONSABILITA'
Dirigente scolastico	la responsabilità generale per i dati e la sicurezza dei dati; garantire che la scuola utilizzi un Internet Service filtrato approvato, conforme ai requisiti di legge vigenti ; la responsabilità di assicurare che il personale riceva una formazione adeguata per svolgere i ruoli di sicurezza on-line e per la formazione di altri colleghi; essere a conoscenza delle procedure da seguire in caso di infrazione della E-Safety Policy; ruolo di primo piano nello stabilire e rivedere la E-Safety Policy; ricevere relazioni di monitoraggio periodiche della sicurezza online da parte del responsabile; garantire che vi sia un sistema in grado di monitorare il personale di supporto che svolge le procedure di sicurezza online interne.
Docenti	illustrare agli studenti il presente documento; dare indicazioni sul corretto uso della rete; supervisionare e guidare gli alunni con cura quando sono impegnati in attività di apprendimento che coinvolgono la tecnologia on-line; garantire che gli alunni siano pienamente consapevoli delle capacità di ricerca e siano pienamente consapevoli dei problemi legali relativi ai contenuti elettronici come ad esempio le leggi sul copyright;

	assicurare la riservatezza dei dati personali trattati ai sensi della normativa vigente.
Alunni	<p>leggere, comprendere, ed accettare la E- Safety Policy ; avere una buona comprensione delle capacità di ricerca e la necessità di evitare il plagio e rispettare normative sul diritto d'autore; capire l'importanza di segnalare abusi, o l'uso improprio o 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 on-line; conoscere e capire la politica relativa all'uso dei telefoni cellulari, fotocamere digitali e dispositivi portatili; non utilizzare i materiali della scuola per scopi personali; non rovinare i devices forniti dalla scuola; non eseguire tentativi di modifica della configurazione di sistema dei dispositivi; conoscere e capire la politica della scuola sull'uso di immagini personali, dei compagni, dei docenti; non diffondere dati personali; capire l'importanza di adottare buone pratiche di sicurezza on-line quando si usano le tecnologie digitali fuori dalla scuola;</p>
Personale ATA	<p>comprendere e contribuire a promuovere politiche di e-sicurezza essere consapevoli dei problemi di sicurezza on-line connessi con l'uso di telefoni cellulari, fotocamere e dispositivi portatili; monitorare l'uso di dispositivi tecnologici e attuare politiche scolastiche per quanto riguarda questi dispositivi; segnalare qualsiasi abuso sospetto o problema ai responsabili della sicurezza online; usare comportamenti sicuri, responsabili e professionali nel l'uso della tecnologia; garantire che le comunicazioni digitali con gli studenti dovrebbero essere a livello professionale e solo attraverso i sistemi scolastici, non attraverso meccanismi personali, per esempio -mail, telefoni cellulari, ecc.</p>
Genitori	<p>sostenere la scuola nel promuovere la sicurezza online e approvare l'accordo di E- Safety Policy con la scuola; partecipare agli incontri proposti dalla scuola relativamente alla sicurezza nell'uso di internet e delle tecnologie digitali e al cyberbullismo; non diffondere dati personali; adottare condotte rispettose degli altri quando si comunica in rete; conoscere le norme di utilizzo della rete nel rispetto del copyright e del diritto di autore; rispettare la normativa relativa alla privacy.</p>

Condivisione e comunicazione della Policy all'intera comunità scolastica

Oltre alla pubblicazione della E-Safety Policy sul sito della scuola, la Policy sarà comunicata al personale, agli alunni, alla comunità nei seguenti modi:

- Condivisione e comunicazione agli alunni:
 - all'inizio dell'anno scolastico in occasione della presentazione del Regolamento d'Istituto;
 - nel corso dell'anno scolastico, con la realizzazione di particolari moduli del curriculum digitale.

- Condivisione e comunicazione al personale:
 - il documento sarà discusso negli organi collegiali;
 - il personale riceverà informazione attraverso materiali pubblicati sul sito della scuola e corsi di formazione.

- Condivisione e comunicazione ai genitori:
 - condivisione del documento nelle assemblee di classe;
 - incontri formativi.

Gestione delle infrazioni alla Policy

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

- utilizzo non corretto della strumentazione della scuola;
- utilizzo del proprio dispositivo (in particolare smartphone) quando non richiesto;
- poca cura o considerazione per i diritti d'autore relativamente a musica e film;
- validazione dei contenuti: come controllare l'autenticità e l'esattezza dei contenuti online;
- bullismo on-line in tutte le forme;
- questioni di privacy, tra cui la divulgazione di informazioni personali o la pubblicazione di foto o immagini non autorizzate e/o compromettenti;
- reputazione online
- la salute e il benessere (quantità di tempo speso online su Internet o giochi)

DA FARE: ufficializzare con l'approvazione del Collegio Docenti il regolamento per l'utilizzo delle attrezzature fornite dalla scuola.

Integrazione della policy con regolamenti esistenti

Il presente documento si integra con gli obiettivi e i contenuti dei seguenti documenti: PTOF e Regolamento d'Istituto.

2. FORMAZIONE E CURRICOLO

CURRICOLO DIGITALE

Il curriculum è stato realizzato tenendo conto del Sillabo di Educazione Civica Digitale pubblicato dal Miur nel 2018.

Infanzia

Cultura e creatività digitale	Tutte le classi	attività di coding unplugged, robotica educativa, coding, scacchi, utilizzo di puzzle Lego.	Annualità	Tutte le aree
-------------------------------	-----------------	---	-----------	---------------

Primaria

Area sillabo ECD	Anno di corso	Contenuti	Tempi	Aree coinvolte
Educazione all'informazione	3°-4°-5°	<ul style="list-style-type: none">- Primi approcci alla sicurezza on-line e alla ricerca in internet	Annualità	Area linguistica e antropologica
Educazione ai media Cultura e creatività digitale	3°-4°-5°	<ul style="list-style-type: none">- Conoscere le prime regole della comunicazione attraverso strumenti digitali: maiuscolo, sintesi, evitare domande ripetitive, linguaggio adeguato...- Comprendere la differenza tra dati personali condivisibili e non- Comprendere che la propria traccia in rete può essere letta da diversi attori, comunicazione non ostile- Comprendere la differenza tra identità reale e identità digitale	Annualità	Trasversale (in particolare area linguistica)

Cultura e creatività digitale	Tutte le classi	<p>Per le classi 1° e 2° attività di coding unplugged, robotica, pixel art, scacchi.</p> <p>Per le classi 3° e 4°</p> <ul style="list-style-type: none"> - Produrre elaborati con linguaggi diversi e supporti digitali (avvio all'uso di programmi di scrittura) - sviluppo del linguaggio computazionale e problem solving attraverso coding e attività varie <p>Per le classi 5°</p> <ul style="list-style-type: none"> - comprendere il significato di "proprietà intellettuale" e rispettarla - introduzione all'uso di power-point, saper salvare in una cartella e stampare un file - sviluppo del linguaggio computazionale e problem solving attraverso coding 	Annualità	Tutte le aree
Quantificazione e computazione: dati e intelligenza artificiale	3°-4°-5°	<ul style="list-style-type: none"> - Saper utilizzare una password per proteggere i propri dispositivi - Riflettere sul potere distraente delle tecnologie rispetto alle relazioni in presenza, a compiti specifici ecc. - Riconoscere, usare e dosare l'utilizzo delle tecnologie digitali senza esserne dipendenti - Riciclare e smaltire correttamente i dispositivi 	Annualità	Tutte le aree
Cultura e creatività digitale	3°-4°-5°	<ul style="list-style-type: none"> - Saper utilizzare semplici software di storytelling (scratch...), editing di immagini, foto e video per documenti di testo e/o presentazioni legate all'attività didattiche 	Annualità	Tutte le aree

Secondaria di 1^ Grado

Area syllabo ECD	Anno di corso	Contenuti	Tempi	Discipline coinvolte
Educazione all'informazione (parte 3)	Primo anno (modulo 1)	Come funzionano i motori di ricerca e vari siti didattici generalisti gestiti da studenti.	4 ore	Lettere
Educare all'informazione.	Primo anno (modulo 2)	Come valutare l'attendibilità, l'aggiornamento di un sito.	4 ore	Lettere Le varie discipline forniscono una sitografia di base per le ricerche (1 ora a disciplina)
Educare all'informazione	Triennio	Costruire cartelle e sottocartelle organizzare e classificare contenuti digitali. Anche in gruppo.	Tutto l'anno scolastico	Area scientifica
Cultura e creatività digitale (parte 5)	Triennio	Come si rielaborano le informazioni (no plagio) Come citare le fonti Come mettere link e creare una sitografia	Tutto l'anno scolastico	Tutte le discipline.
Cultura e creatività digitale	Triennio	Come lavorare su un file condiviso	Tutto l'anno scolastico	Tutte le discipline
Cultura e creatività digitale	Triennio	Creazione di presentazioni, fogli di calcolo, conoscenza e uso di web-app, ecc. Social reading	Tutto l'anno scolastico	Tutte le discipline.
Cultura e creatività digitale	Triennio	Creazione di video, podcast...	Tutto l'anno scolastico	Tutte le discipline.
Cultura e creatività digitale	Triennio	Coding, pensiero computazionale Robotica	Tutto l'anno scolastico	Tutte le discipline.
Educazione ai media (parte 2)	Triennio	Conoscenza dei rischi della rete Elementi normativi sulla tutela della privacy Normativa di base sull'utilizzo dei social network Approfondimento dei concetti di netiquette, flame, tag...		Possibili interventi di esperti esterni (polizia postale, avvocati, psicologi...

PREREQUISITI RICHIESTI DALLA SCUOLA SECONDARIA DI PRIMO GRADO

- 1.1 Introduzione al concetto della proprietà intellettuale/diritti di autore per lavorare con musica, immagini e i testi reperibili in internet
- 1.3 Semplice organizzazione di file in cartelle
- 2.5 Conosce le norme di comportamento nei confronti dei compagni anche in ambito digitale (comunicazione non ostile, lessico appropriato, rispetto...)

- 3.1 Creazione e salvataggio di un semplice documento di testo (editing, impaginazione di un'immagine)
- 3.4 Coding unplugged, approccio al pensiero computazionale
- 4.2 Capire che devono proteggere i dati personali e la propria immagine (no diffusione, no iscrizione on-line senza la presenza di un genitore)

Formazione dei docenti sull'utilizzo e l'integrazione delle TIC nella didattica e sull'utilizzo consapevole e sicuro di internet delle tecnologie digitali

Le attività di formazione previste per i docenti sono:

- formazione promossa dal Miur per Animatore Digitale e Team per l'innovazione;
- autoformazione interna;
- corsi di formazione organizzati dall'Istituto.

Sensibilizzazione delle famiglie

L'Istituto sta definendo un protocollo di incontri, tenuti da esperti o da docenti formati, da attuare annualmente per sensibilizzare le famiglie su cyberbullismo e uso consapevole della rete e delle tecnologie digitali

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

L'accesso ad internet avviene attraverso rete fissa o attraverso wi-fi, in questo caso si accede attraverso una procedura di autorizzazione che richiede una password.

Nel computer portatili si accede attraverso una password e in tutti i computer l'installazione dei programmi è riservata all'amministratore.

Sui computer sono installati programmi antivirus. Anche la navigazione in internet è controllata.

Sito web della scuola

La scuola ha un sito web del quale è responsabile. La scuola, in qualità di ente pubblico, pubblicherà sul proprio sito web i contenuti che saranno valutati come pertinenti alle finalità educative istituzionali, ponendo attenzione alla tutela della privacy degli studenti e del personale, secondo le disposizioni normative.

La scuola ha una pagina Facebook gestita dall'Animatore Digitale e da alcuni membri del Team.

Si usa da alcuni anni il registro elettronico.

Protezione dei dati personali

I dati personali sono protetti secondo la normativa vigente, viene richiesta specifica autorizzazione per l'utilizzo di foto, video, testi per la documentazione di attività didattiche, anche in occasione di eventi o manifestazioni, e per la pubblicazione sul sito della scuola e/o blog scolastici.

4. STRUMENTAZIONE PERSONALE

Per gli studenti:

Come da Regolamento d'Istituto agli studenti è vietato l'utilizzo del cellulare all'interno della scuola.

No è richiesto l'uso di altra strumentazione personale.

Per i docenti e per il personale della scuola :

I docenti e il personale della scuola possono utilizzare i propri cellulari in orario di lavoro solo per emergenze.

I docenti possono usare i propri devices per scopi didattici a integrazione dei dispositivi scolastici a disposizione.

5. PREVENZIONE, RILEVAZIONE E GESTIONE DEI CASI

La scuola avrà cura di inserire nel curriculum digitale attività finalizzate alla prevenzione di comportamenti a rischio quali cyberbullismo, adescamento on-line, sexting, pornografia, gambling, dipendenza da internet, esposizione a contenuti inadeguati e dannosi.

Prevenzione Principi generali:

1. Internet favorisce la libertà d'espressione e, quando si entra a far parte di una community o di un servizio dove interagiscono più utenti, vanno considerati abusi meritevoli di segnalazione solo i contenuti palesemente impropri o illeciti e non tutti quei contenuti con cui semplicemente non si è d'accordo o non piacciono.

2. Quando si inizia a navigare tra i servizi dei Social Network e le applicazioni web tipo YouTube, Facebook, etc., bisogna informarsi subito su quali sono i diritti e i doveri dell'utente, leggendo il regolamento, tenendosi aggiornati, esplorando i siti informativi e istituzionali che affrontano queste tematiche.

3. Se si condividono informazioni personali, bisogna farlo scegliendo con cura che cosa rendere pubblico e cosa rendere privato. E' indispensabile scegliere con attenzione le amicizie con cui accrescere la propria rete e i gruppi a cui aderire, proteggendo la propria identità digitale con password complesse e usando una domanda di recupero password dalla risposta non banale.

4. Se si condividono elementi multimediali o informazioni che riguardano più persone è necessario avere il permesso di ciascun utente coinvolto prima di effettuare la pubblicazione. Non bisogna pubblicare su YouTube video girati di nascosto e dove sono presenti persone filmate senza il loro consenso.

5. Bisogna contribuire a rendere il Web un luogo sicuro, pertanto ogni volta che un utente commette involontariamente un abuso o un errore, pubblicando del materiale illecito, non idoneo o offensivo, bisogna contattarlo e fornire le spiegazioni relative alle regole, diffondendo così i principi della sicurezza.

6. Ogni abuso subito o rilevato nella navigazione, deve essere segnalato tramite i canali e gli strumenti offerti dal servizio, indicando in modo semplice i riferimenti per ottenere tempestivamente la rimozione del contenuto (abuso, data, ora, utenti e servizio coinvolti). Tutti i social network garantiscono la possibilità di segnalare materiale inopportuno mediante semplici operazioni da compiere direttamente sul sito. Prima di trasformare un incidente o una "bravata" in una denuncia alle autorità competenti avvalersi della modalità di segnalazione che non obbliga le parti in causa a conseguenze penali e giudiziarie che possono durare anni.

Scuola e Famiglia possono essere determinanti nella diffusione di un atteggiamento mentale e culturale che consideri la diversità come una ricchezza e che educi all'accettazione, alla consapevolezza dell'altro, al senso della comunità e della responsabilità collettiva.

Occorre, pertanto, rafforzare e valorizzare il Patto di Corresponsabilità educativa previsto dallo Statuto delle studentesse e degli studenti della Scuola Secondaria: la scuola è chiamata ad adottare misure atte a prevenire e contrastare ogni forma di violenza e di prevaricazione;

la famiglia è chiamata a collaborare, non solo educando i propri figli ma anche vigilando sui loro comportamenti.

Per definire una strategia ottimale di prevenzione e di contrasto, le esperienze acquisite e le conoscenze prodotte vanno contestualizzate alla luce dei cambiamenti, che hanno profondamente modificato la società sul piano etico, sociale e culturale e ciò comporta una valutazione ponderata delle procedure adottate per riadattarle in ragione di nuove variabili, assicurandone in tal modo l'efficacia.

Azioni

I docenti si impegnano a:

- accompagnare gli alunni nella navigazione in Rete, coinvolgendoli nell'esplorazione delle opportunità e dei rischi, con attività calendarizzate dall'inizio dell'anno;
- approfondire, con attività mirate in classe, la conoscenza del fenomeno del bullismo e del cyber bullismo;
- creare degli spazi in cui gli alunni si possano confrontare su questo tema, utilizzando come spunti di riflessione: spezzoni di film, canzoni, materiali prodotti da altri alunni coinvolti nel progetto SIC;

- confrontarsi con gli altri insegnanti della classe, della scuola o con esperti del territorio;
- rivolgersi alla helpline di generazioni connesse (www.generazioniconnesse.it).

-

I genitori si impegnano a :

- firmare il patto di Corresponsabilità redatto dalla scuola;
- prendere visione della E-Safety Policy;
- seguire le azioni promosse dalla scuola per un uso corretto della rete;
- frequentare corsi di formazione/convegni che la scuola organizzerà per la diffusione di informazioni legate ad un uso corretto della tecnologia digitale.

Gli alunni si impegnano a :

- prendere visione della E-Safety Policy pubblicata sul sito web della scuola; rispettare le regole per un uso corretto della tecnologia;
- denunciare qualsiasi caso di abuso online;
- prendere parte a qualsiasi evento che la scuola organizza in materia di sicurezza online.

Rilevazione e gestione dei casi

Questa parte, oggetto di lavoro nel presente anno scolastico, è in fase di definizione, tenendo conto di quanto appreso in corsi di formazione frequentati recentemente da alcuni docenti del Team digitale.