

Istituto Comprensivo “Marco Emilio Lepido”

Via Premuda, 34 - Reggio Emilia

<http://www.iclepido.edu.it/>

E-Safety Policy

INDICE

1. Introduzione

- Scopo della Policy.
- Ruoli e Responsabilità (*che cosa ci si aspetta da tutti gli attori della Comunità Scolastica*).
- Condivisione e comunicazione della Policy all'intera comunità scolastica, monitoraggio.
- Gestione delle infrazioni alla Policy.
- Integrazione della Policy con Regolamenti esistenti.

2. Formazione e Curricolo

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

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

- Accesso ad internet: filtri, antivirus e navigazione.
- Identità digitale
- Blog e sito web della scuola
- Protezione dei dati personali.

4. Strumentazione personale

- Per gli studenti: gestione degli strumenti personali - cellulari, tablet ecc..
- Per i docenti: gestione degli strumenti personali - cellulari, tablet ecc..
- Per il personale della scuola: gestione degli strumenti personali - cellulari, tablet ecc.

5. Prevenzione, rilevazione e gestione dei casi

Prevenzione

Rilevazione

Gestione dei casi

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

Annessi (da prodursi a cura della scuola)

1. Procedure operative per la gestione delle infrazioni alla Policy.
2. Procedure operative per la protezione dei dati personali.
3. Procedure operative per la rilevazione, il monitoraggio e la gestione delle segnalazioni.
4. Procedure operative per la gestione dei casi.
5. Protocolli siglati con le forze dell'ordine e i servizi del territorio per la gestione condivisa dei casi.

1. INTRODUZIONE

1.1. Scopo della policy.

In riferimento al piano d'azione prodotto dalla scuola che individua le principali aree di intervento in materia di sicurezza e di cultura digitale, l'I.C. "Marco Emilio Lepido" di Reggio Emilia procede alla stesura di un documento di e-policy che si applica a tutti coloro che a vario titolo appartengono e frequentano la scuola e sono pertanto fruitori dei sistemi e delle infrastrutture informatiche.

In modo più specifico esso ha lo scopo di disciplinare il comportamento degli alunni, attraverso interventi di sensibilizzazione e informazione, relativamente all'adozione di comportamenti digitali corretti e appropriati, che possano essere estesi anche ad ambiti extrascolastici.

Si pone pertanto come documento di riferimento che autorizza il Dirigente scolastico e il personale docente a stabilire sanzioni disciplinari per comportamenti inappropriati avvenuti all'interno dell'istituzione scolastica.

L'Istituto Comprensivo svolge inoltre attività di formazione, prevenzione e vigilanza sugli alunni, promuovendo specifici progetti in un'ottica di confronto e dialogo con le famiglie, con lo scopo di creare un terreno favorevole alla crescita di cultura e cittadinanza digitale, con l'auspicio di ridurre il più possibile l'occorrenza di atti che non solo creano conflitti e disagio all'interno della comunità scolastica, ma possono anche in taluni casi configurarsi come reati.

Per rispondere a tali bisogni educativi la scuola opera in stretta collaborazione con le forze dell'ordine, la Procura della Repubblica, il Tribunale dei minori, i Servizi sociali e le istituzioni del settore educativo sul territorio, per mettere in campo strategie di prevenzione al cyber-bullismo e realizzare interventi di recupero nel caso in cui si verificano tali situazioni.

1.2. Ruoli e responsabilità (che cosa ci si aspetta da tutti gli attori della comunità scolastica).

<u>Il Dirigente Scolastico</u>	<p>È responsabile della revisione di questo documento ponendolo all'attenzione del Consiglio di Istituto e del Collegio Docenti.</p> <p>Deve inoltre, in collaborazione con il referente della sicurezza on-line, valutarne l'efficacia e monitorarne l'attuazione.</p> <p>Mette in atto le misure preposte a garantire la tutela degli aspetti legali riguardanti la privacy e la tutela dell'immagine di tutti i membri della comunità scolastica; a questo scopo è fondamentale che riceva tempestive e puntuali informazioni da parte del corpo docente o del personale ATA o da chiunque sia giunto a conoscenza di eventuali violazioni al presente regolamento.</p>
--------------------------------	--

<p><u>Docente referente della sicurezza on-line</u> (su nomina del D.S.)</p>	<p>È un docente che ha svolto una specifica formazione sulle tematiche citate, opera in stretta collaborazione con il Dirigente scolastico, l'animatore digitale e il team digitale per promuovere comportamenti di consapevolezza e sicurezza online in tutta la comunità scolastica.</p> <p>Facilita le procedure di gestione delle infrazioni tenendo un registro di incidenti di sicurezza online; collabora alla formazione dei colleghi ed è punto di riferimento per la consulenza per tutto il personale.</p> <p>Coordina gli interventi di prevenzione e gestione di eventuali azioni di cyberbullismo in stretta collaborazione con il Dirigente Scolastico, le autorità locali e le agenzie competenti.</p>
<p><u>L'animatore digitale</u></p>	<p>Opera in stretta collaborazione con il D.S., il docente referente per la sicurezza on line e con i docenti del team digitale, curando la redazione e la revisione annuale del documento di e-policy sulla base delle osservazioni ricevute da tutti i soggetti interessati; favorisce la massima diffusione dello stesso all'interno della comunità scolastica in tutte le sue componenti (docenti, ata, genitori e studenti).</p> <p>Promuove azioni di formazione interna alla scuola negli ambiti del PNSD, attraverso l'organizzazione di corsi e laboratori formativi, favorendo il confronto e la partecipazione di tutta la comunità scolastica.</p> <p>Si relaziona con la ditta che gestisce l'assistenza tecnico informatica per definire le misure di sicurezza più opportune.</p> <p>Riferisce al Dirigente Scolastico situazioni o problemi di particolare rilevanza su cui intervenire.</p>
<p><u>Il personale docente</u></p>	<p>È tenuto ad avere adeguata consapevolezza circa le questioni di sicurezza informatica e relative buone pratiche.</p> <p>È tenuto a conoscere e sottoscrivere la presente policy, contribuendo alla sua attuazione attraverso la segnalazione di qualsiasi abuso, anche sospetto, al Dirigente Scolastico per le opportune indagini.</p> <p>Si impegna a mantenere le comunicazioni digitali con alunne/alunni e famiglie a livello professionale e realizzarle attraverso sistemi ufficiali scolastici.</p>

	<p>Ha un ruolo educativo determinante nel far comprendere e mettere in pratica le regole di comportamento relative alla sicurezza informatica.</p> <p>Nell'utilizzare internet e i linguaggi digitali è tenuto a promuovere attività didattiche finalizzate a un uso responsabile e opportuno del Web che comprenda anche le capacità di discriminare tra siti attendibili e leciti, da quelli illeciti e ingannevoli, in modo da favorire la crescita di consapevolezza e di competenza digitale evitando il plagio e l'indebita diffusione di dati personali.</p> <p>Riconosce pertanto l'importanza della formazione e dell'autoformazione in materia.</p>
<p><u>Il personale ATA</u></p>	<p>Il personale ATA è tenuto a:</p> <ul style="list-style-type: none"> - aver letto, compreso e sottoscritto la presente policy; - collaborare con il personale docente segnalando qualsiasi abuso, anche sospetto, ai docenti responsabili, al Dirigente Scolastico o al docente referente per le opportune verifiche del caso. - mantenere tutte le comunicazioni digitali con alunne/alunni e genitori/tutori a livello professionale e realizzarle esclusivamente con sistemi ufficiali scolastici.
<p><u>Le alunne/gli alunni</u></p>	<p>Sono responsabili dell'utilizzo corretto delle tecnologie digitali e delle infrastrutture informatiche coerentemente con quanto previsto da questa policy. In particolare sono tenuti a:</p> <ul style="list-style-type: none"> - evitare l'utilizzo di dispositivi digitali personali durante le attività didattiche se non espressamente consentito dal personale docente, previa motivazione e finalità didattica; <ul style="list-style-type: none"> - considerare le potenzialità e le opportunità di una valida e corretta ricerca sul web, evitando il plagio, prestando attenzione a non diffondere dati personali propri e altrui; - comprendere l'importanza della segnalazione di ogni abuso, uso improprio o accesso a materiali inappropriati e conoscere il protocollo per tali segnalazioni; <ul style="list-style-type: none"> - essere consapevoli del significato e della gravità di atti di cyber-bullismo, evitando i ruoli attivi, ma anche quelli di testimoni passivi a danni di terzi - capire l'importanza di adottare buone pratiche di sicurezza informatica in tutti i momenti della vita, a tutela dell'incolumità propria e altrui per evitare di commettere infrazioni o reati punibili sia a livello scolastico sia da parte della magistratura.

<u>I Genitori</u>	<p>Svolgono un ruolo cruciale nel garantire che i loro figli comprendano la necessità di utilizzare i dispositivi Internet e mobili in modo appropriato.</p> <p>Saranno perciò invitati a contribuire, in sinergia con il personale scolastico, alla sensibilizzazione dei propri figli sul tema della sicurezza in rete, incoraggiando l'impiego del digitale anche nello svolgimento dei compiti a casa, controllando che tale impiego avvenga nel rispetto delle norme di sicurezza.</p> <p>Il loro supporto sarà fondamentale nell'agire in modo concorde alla scuola per la prevenzione dei rischi e l'attuazione delle procedure previste in caso di violazione delle regole stabilite.</p>
-------------------	---

1.3. Condivisione e comunicazione della policy all'intera comunità scolastica, monitoraggio.

Il presente documento verrà pubblicato sul sito Web della scuola e verrà annualmente valutata la necessità di operare modifiche.

Per favorire la condivisione e la comunicazione del documento all'interno della comunità scolastica si indicano di seguito alcune azioni e iniziative:

Per il corpo docente:

- Discussione collegiale sui contenuti, (anche nella modalità di autoformazione) sulle pratiche indicate e su come inserire nel curriculum le tematiche di interesse della policy; si auspica un confronto collegiale, su base annuale, circa la necessità di apportare modifiche e miglioramenti alla policy vigente;

Per la componente studentesca:

- Discussione in classe della policy, unitamente al regolamento di istituto nel primo periodo di frequenza scolastica e durante le procedure di accoglienza delle nuove classi prime;
- Inserimento di un estratto del documento di e-policy nel diario scolastico e in particolare delle procedure relative ai comportamenti da seguire.
- Discussione con attività mirate del documento di e-policy per le classi seconde e terze

Per i genitori:

- Condivisione e confronto all'interno del Consiglio di Istituto del documento di e-policy
- Diffusione e condivisione del documento all'interno delle assemblee di classe
- Organizzazione di incontri di sensibilizzazione sui temi di cittadinanza digitale e di sicurezza on line, informazione circa i comportamenti da monitorare o da evitare.

1.4. Gestione delle infrazioni della policy.

A partire dall'entrata in vigore di questo documento si costituisce un gruppo di *e-safety* d'Istituto, composto dal docente referente per la sicurezza online, dall'animatore Digitale e dai membri del team del PNSD e da un docente indicato dal collegio della scuola primaria che abbia svolto formazione nell'ambito delle tematiche previste dal PNSD.

Tale gruppo, in costante collaborazione col D.S., ha l'incarico di supportare il docente referente della sicurezza online nel monitorare la situazione, aggiornando il documento di e-policy ed esaminando la traccia delle segnalazioni nell'apposito *Diario di Bordo* di Generazioni Connesse, che diventa strumento ufficialmente adottato dalla scuola per archiviare le informazioni fondamentali sulle segnalazioni (data e ora, azioni intraprese, insegnante responsabile della segnalazione, ecc.. vedi allegato n. 3).

1.5. Integrazione della policy con Regolamenti esistenti.

La presente policy viene pubblicata sul sito Web istituzionale della scuola e si integra al Regolamento di Istituto, al PTOF, e al **Piano scolastico della DDI** redatto quest'anno scolastico in conformità con le [linee guida emanate dal MIUR il 7.08.'20](#)

2. FORMAZIONE E CURRICOLO

2.1 Curricolo sulle competenze digitali per gli studenti.

Nelle "Linee di orientamento per azioni di prevenzione e contrasto al bullismo e al cyberbullismo" il Miur sottolinea l'importanza di far comprendere agli studenti che la propria e altrui sicurezza sul Web non dipendono solo dalle tecnologie adottate, ma anche dalla capacità di discernimento delle singole persone. In quest'ottica si colloca anche il Piano Nazionale Scuola Digitale che individua (azione 14) alcuni *framework* di riferimento per lo sviluppo delle competenze digitali.

Tra questi il PNSD fa esplicito riferimento al *framework* **DigComp** (Quadro delle competenze Europee Digitali per i Cittadini), strumento pubblicato nel 2013 e aggiornato nel 2016 finalizzato a migliorare la competenza digitale dei cittadini, che viene dunque preso a riferimento per la definizione del curricolo sulle competenze digitali del nostro istituto.

<http://www.cittadinanzadigitale.eu/wp-content/uploads/2016/07/DigComp-2.0.pdf>

La nuova versione evidenzia l'evoluzione delle competenze digitali in relazione alle tendenze emergenti, alle quali anche la nostra scuola sta cercando di dare risposta:

- l'impiego diffuso del cloud per l'archiviazione di dati e contenuti,
- l'importanza crescente delle competenze di data literacy,
- gli aspetti legati all'accessibilità, all'inclusione sociale, alla privacy e alla protezione dei dati personali.

Si configura dunque un nuovo ed evoluto concetto di *competenza digitale* che può essere declinato come "uso creativo delle tecnologie digitali per creare conoscenza e innovare processi e prodotti." (DigComp 2.0)

Si fa inoltre riferimento al modello sviluppato dal gruppo di lavoro del Prof. Antonio Calvani che ha

formulato un quadro di riferimento sulle competenze digitali¹ riconducibile a tre dimensioni principali, all'interno delle quali anche la nostra scuola ha individuato specifiche abilità richieste:

1. Dimensione tecnologica:

- selezionare la tecnologia adeguata per ciascun compito
- identificare i problemi tecnici durante l'utilizzo dei dispositivi o degli ambienti digitali e indicare le possibili soluzioni
- operare logicamente
- rappresentare processi simbolici

2. Dimensione cognitiva:

- saper valutare la pertinenza e la veridicità dell'informazione
- saper trattare le informazioni (sintetizzare, rappresentare, analizzare) producendo testi, dati, tabelle e grafici ad esse relativi.
- saper integrare informazioni e contenuti già dati in modo creativo e pertinente, contribuendo alla diffusione di nuove conoscenze

3. Dimensione etica:

- conoscere i concetti di tutela della privacy
- rispettare i diritti intellettuali dei materiali reperiti in Internet e l'immagine degli altri
- comprendere il dislivello sociale e tecnologico che può esistere tra paesi, persone, generazioni

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

Il piano di formazione di Istituto prevede due principali ambiti di intervento:

- Una formazione organizzata dal Miur che si svolge secondo le modalità e i tempi previsti dal PNSD e che si realizza attraverso gli snodi formativi;
- Una formazione interna all' istituto, con formatori esterni o interni nella modalità di tutoring/laboratorio. Questo tipo di intervento si basa sulle esigenze formative espresse dai docenti, rilevate ad inizio d'anno dall'animatore digitale e dal team del PNSD e mirate all'integrazione delle TIC nelle proposte didattiche dei docenti.

A partire dal mese di settembre 2020 sono state organizzate attività di formazione sulla didattica digitale rivolte a tutti i docenti dell'istituto per moduli tematici anche differenziati sulla base delle competenze dei docenti. Ogni docente ha svolto un numero minimo di 6 ore di formazione equivalenti alla frequenza di 3 moduli, privilegiando le seguenti tematiche:

- Piattaforma G Suite for Education
- Metodologie innovative di insegnamento (didattica breve, l'uso dei video nella didattica, flipped classroom)

¹ Il quadro di riferimento delle competenze digitali dovrà tenere in adeguata considerazione il principio di gradualità nelle diverse aree di apprendimento, anche in riferimento al percorso scolastico e ai diversi ordini di scuola.

- Si allega il [piano di formazione](#) per il mese di settembre e ottobre

2.3 Sensibilizzazione delle famiglie.

Il nostro istituto organizza incontri aperti alle famiglie e agli studenti in collaborazione con enti esterni, come la Polizia Postale, per sensibilizzare docenti, alunni e genitori sui temi della sicurezza online.

Si prevede inoltre, unitamente alla diffusione e alla condivisione di questo documento (nelle modalità descritte al punto 1.3) di favorire l'accessibilità e la diffusione dei materiali dedicati alle famiglie disponibili nella bacheca virtuale del sito "*Generazioni connesse*" per favorire una riflessione sui temi della cittadinanza digitale e della prevenzione dei rischi legati a un uso improprio e scorretto del Web.

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

3.1. Accesso ad internet: filtri, antivirus e navigazione.

La connettività a Internet è possibile in tutti i plessi dell'Istituto comprensivo tramite rete locale LAN, in tutti gli ambienti didattici e amministrativi, oppure tramite WIFI protetto da password. La connettività dell'istituto è stata ampliata grazie alla partecipazione ai bandi PON LAN-WLAN 2014-2020 e recentemente implementata negli spazi in cui il segnale risultava più debole.

L'accesso ad Internet è finalizzato ad esigenze didattiche così da permettere a studenti e docenti di fruire di risorse utili nella ricerca e nella produzione di contenuti digitali autentici, e ad esigenze amministrative, per l'espletamento di pratiche burocratiche, oltre che per consentire le attività di didattica digitale integrata determinate dalla pandemia.

La Scuola promuove e adotta opportuni accorgimenti per evitare comportamenti contrari alle norme di sicurezza informatica, attraverso una manutenzione scrupolosa delle infrastrutture di rete in collaborazione con la ditta che cura l'assistenza tecnica, aggiornando antivirus e intervenendo sia periodicamente che nei casi di emergenza.

Nella pratica didattica, il docente ha un ruolo fondamentale di responsabilità nel favorire l'uso corretto della rete, guidando gli studenti nelle attività online, stabilendo obiettivi chiari di ricerca, insegnando le strategie appropriate nella definizione e nella gestione delle risorse digitali su Web.

3.2. Identità digitale

Accogliendo le indicazioni del PNSD in materia di identità digitale, la scuola ha adottato la G-suite FOR EDUCATION che consente accessi individualizzati per tutti i soggetti coinvolti nella comunità scolastica (studenti, docenti, ATA).

Questo si è rivelato particolarmente utile sia per gli aspetti amministrativi e gestionali che nelle comunicazioni tra docenti e alunni e diviene risorsa essenziale nelle diverse situazioni di didattica digitale integrata che si applicano a causa dell'emergenza sanitaria.

L'account studente e l'account docente ha inoltre reso possibile la creazione di archivi di materiali sempre accessibili e modificabili e ha permesso la creazione di ambienti virtuali di apprendimento (classi virtuali) che favoriscono e facilitano la crescita delle competenze digitali degli studenti.

3.3. Blog e sito web della scuola

Il sito web della scuola (<http://www.iclepidogov.it/>) è gestito dalla cooperativa *Scuola Online Service* che ne cura la parte amministrativa garantendo l'accessibilità e la conformità alla normativa vigente. Il personale della segreteria, per il settore amministrativo scolastico e alcuni insegnanti (animatore digitale e referenti specifici progetti) per il settore didattico, partecipano all'implementazione del sito in qualità di editor aggiornando le pagine nelle rispettive sezioni di riferimento.

Dalla home page mediante login protetto da password o direttamente dalla home page della piattaforma i docenti possono accedere alla compilazione del registro elettronico online *Nuvola* di Madisoft.

Da questo anno scolastico è inoltre attiva la pagina facebook di istituto gestita da un docente referente supportato da una commissione di insegnanti appartenenti ai diversi plessi dell'istituto (primaria e secondaria). La pagina si prefigge scopi di documentazione delle attività didattiche interne alla scuola, dando particolare rilievo (grazie alle caratteristiche del canale di comunicazione) alle attività dell'indirizzo musicale.

Per specifici progetti didattici utilizzando il dominio *.edu* e l'applicazione *Site* della G-suite for Education sono stati elaborati alcuni blog tematici con il contributo degli alunni di diverse classi coordinati dai docenti e dall'animatore digitale. Fra questi nell'a.s. 2016-'17 è stato elaborato un blog dal titolo "*A prova di bullo!*" che ha visto la pubblicazione di un podcast sul tema del bullismo e del cyberbullismo. Il progetto ha coinvolto cinque classi terze e una classe seconda.

Nell'a.s. 2017/'18 il sito sopracitato è stato ampliato con l'inserimento di nuovi contenuti digitali (video, infografiche, presentazioni) prodotti dagli studenti e ispirati alle attività suggerite dal sito <https://www.generazioniconnesse.it>. La nuova versione del sito Web è stata illustrata a fine anno scolastico durante un evento pomeridiano rivolto ai genitori.

Link al sito:

https://sites.google.com/a/iclepidogov.it/a_prova_di_bullo/

Nell'anno scolastico 2018/19 si è svolto un progetto di istituto (scuola primaria e secondaria) che per gradi diversi di complessità ha affrontato i temi della comunicazione non ostile e l'uso del pensiero critico nel valutare le fonti informative. La documentazione delle attività è stata raccolta e pubblicata su un sito web tematico e illustrata alle famiglie nel corso di un evento organizzato nel mese di maggio.

Link al sito:

<https://sites.google.com/iclepidogov.it/saravero-curiosiperpassione>

Nell'anno scolastico 2019/20 il progetto di istituto di educazione alla cittadinanza caratterizzato da approfondimenti sul tema del senso delle regole, si è in parte modificato in corso in un'ottica di condivisione e dialogo con le famiglie. In alcune classi verranno sviluppate unità didattiche sulla conoscenza e sul senso delle regole in Internet e sulla necessità di attenersi a comportamenti improntati a sicurezza e correttezza nelle relazioni online. Quanto emerso nel corso delle attività didattiche sarà spunto per la discussione e il confronto nel corso di incontri con i genitori.

Nell'anno scolastico 2020/'21 il collegio ha lavorato alla costruzione di un curricolo verticale di educazione civica all'interno del quale viene dedicato ampio spazio alle tematiche e alle attività legate all'educazione alla cittadinanza digitale.

3.4. Protezione dei dati personali (da cambiare secondo la nuova legge sulla privacy)

Per quanto attiene al tema della protezione dei dati personali il presente documento di e-policy fa riferimento a quanto contenuto nel Regolamento UE 2016/679 per il trattamento di dati personali di alunni e familiari.

Tutto il personale riceve istruzioni dettagliate applicabili al trattamento di dati personali ai fini della protezione e sicurezza degli stessi e in generale si attiene ai seguenti principi:

- Le fotografie o i video da pubblicare sul sito che includano gli studenti saranno selezionati con attenzione preferendo fotografie o video di gruppo piuttosto che foto integrali di singoli.
- I nomi completi di alunne e alunni saranno evitati sul sito web come pure nei blog, in particolare se in associazione alle loro fotografie.
 - All'atto dell'iscrizione è richiesto alle famiglie di firmare un'informativa scritta per consentire l'uso didattico di immagini e video dei minori secondo i principi sopra indicati.
 - Nel caso di eventi speciali, questi verranno presi in considerazione in modo da stabilire l'opportunità di pubblicare dati personali, in tal caso sarà presentata apposita richiesta circostanziata con valide motivazioni che varrà solo per lo specifico evento.

4. STRUMENTAZIONE PERSONALE

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

Gli alunni si impegnano a tenere spenti e a non lasciare incustoditi i telefoni cellulari e i dispositivi digitali mobili. In caso di urgenza per comunicazioni tra gli alunni e le famiglie, su autorizzazione dei docenti e sotto il diretto controllo dei collaboratori scolastici, gli alunni potranno comunicare con le famiglie tramite gli apparecchi telefonici della scuola. Gli alunni possono, dietro esplicito consenso dei docenti, utilizzare i propri dispositivi digitali per finalità didattiche attenendosi strettamente alle indicazioni di lavoro ricevute.

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

Durante le lezioni i docenti utilizzano i dispositivi personali per finalità didattiche e per accedere al registro elettronico ad integrazione dei dispositivi scolastici disponibili. Possono utilizzare i propri strumenti nelle aule e nei laboratori anche al pomeriggio usufruendo dell'impianto wifi d'istituto per attività di studio, ricerca e per la preparazione di compiti e materiali didattici.

Non è loro consentito l'utilizzo degli strumenti personali in classe durante le lezioni per motivi personali, fatto salvo eccezionali episodi a carattere di urgenza.

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

Durante l'orario di servizio al personale scolastico che non rientra nella categoria dei docenti è permesso l'uso del cellulare solo per comunicazioni a carattere d'urgenza.

L'uso di altri dispositivi elettronici personali o di istituto è permesso per attività funzionali al servizio.

5. PREVENZIONE, RILEVAZIONE E GESTIONE DEI CASI

5.1. Prevenzione

La prevenzione dei comportamenti inappropriati in rete, in particolare quelli legati al fenomeno del cyberbullismo, costituisce un processo delicato e complesso che va affrontato tenendo in considerazione una molteplicità di fattori.

Di seguito si individuano i principi guida fondamentali che si ritiene debbano caratterizzare la fase di prevenzione:

- creare un clima di relazioni positive fra i pari e di fiducia negli adulti
- favorire la crescita delle competenze digitali, (graduate per fasce di età) mediante attività didattiche ed educative che promuovano negli studenti il senso di responsabilità del ruolo di cittadini digitali nella società
- attuare progetti e attività didattiche sui temi del cyberbullismo e della sicurezza in rete offrendo opportunità di dialogo e di confronto
- promuovere iniziative di formazione dei docenti
- promuovere iniziative di sensibilizzazione rivolte ai genitori sul tema delle opportunità offerte dal digitale ma anche dei rischi a cui sono esposti i ragazzi che utilizzano la rete in modo del tutto incontrollato
- attivare progetti di peer-education (scuola secondaria) sui temi della sicurezza on line, che comprendano fasi di preparazione e formazione degli studenti

5.2. Rilevazione

Il clima di collaborazione e di disponibilità all'ascolto sono condizioni necessarie per un'efficace rilevazione di comportamenti inadeguati, così come di eventuali situazioni di disagio, in un'ottica di condivisione con le famiglie.

In sintesi si elencano le azioni fondamentali individuate a tale scopo:

- Attivazione di uno sportello di ascolto con il docente referente rivolto ad alunni, famiglie, docenti
- Elaborazione di questionari di monitoraggio generale (scuola secondaria) volti a rilevare il livello di conoscenza delle tematiche relative alla sicurezza online, ma anche finalizzati ad accertare eventuali e specifici episodi vissuti, offrendo così opportunità di dialogo
-

5.3. Gestione dei casi

Anche nel descrivere questa fase si sottolinea l'importanza dell'approccio educativo che vede nella sanzione non la sola stigmatizzazione dei comportamenti inadeguati, ma soprattutto l'opportunità formativa, in un'ottica di crescita dei comportamenti di cittadinanza digitale responsabile.

Nella tabella seguente si descrivono le principali azioni da intraprendere e si definiscono le sanzioni in base alla gravità dei casi e all'età degli alunni coinvolti.

Comportamenti	Azioni da intraprendere
Navigazione su siti non finalizzati all'attività didattica durante le lezioni	Intervento dell'insegnante, sanzione a sua discrezione o del CdC, proporzionata alla gravità dell'infrazione con eventuale comunicazione alla famiglia.
Uso non autorizzato del telefono cellulare (o altri dispositivi) durante le lezioni	Intervento dell'insegnante e ritiro del dispositivo. Comunicazione e riconsegna ai genitori. Eventuali sanzioni e provvedimenti disciplinari a discrezione dell'insegnante o del CdC in caso di comportamenti reiterati
Appropriarsi delle credenziali altrui di istituto (o di identità digitali diverse dalla propria) e alterare o eliminare deliberatamente i dati di qualcuno	Intervento dell'insegnante e sanzione a sua discrezione o del CdC proporzionata alla gravità dell'infrazione e comunicazione alla famiglia.
Acquisire e/o diffondere immagini o video non autorizzati di compagni e personale scolastico	Comunicazione al referente e al Dirigente. Convocazione del CdC e sanzione disciplinare. Comunicazione alla famiglia
Produrre e diffondere materiale ritenuto offensivo, diffamatorio, razzista o violento nei confronti di compagni e personale scolastico	Comunicazione al referente e al Dirigente. Convocazione del CdC e sanzione disciplinare. Comunicazione alla famiglia. Eventuale coinvolgimento della polizia postale

Annessi (da prodursi a cura della scuola)

1. Procedure operative per la protezione dei dati personali.

- Informativa ex artt. 13 e 14 del regolamento UE 2016/679 per il trattamento dei dati personali di alunni e familiari
- Procedure operative per la gestione delle infrazioni alla Policy.
- [Modulo di segnalazione delle infrazioni](#)

2. Procedure operative per la rilevazione, il monitoraggio e la gestione delle segnalazioni.

- [Diario di bordo delle segnalazioni](#)

3. Protocolli siglati con le forze dell'ordine e i servizi del territorio per la gestione condivisa dei casi.
 - Non vi sono protocolli siglati ma ricorrenti forme di collaborazione nella prevenzione e contrasto del bullismo e del cyberbullismo.

Reggio Emilia, 28 Ottobre 2021

L'animatore digitale
Prof.ssa Mariafrancesca Gabbi

Il docente referente della sicurezza on line
Prof. Stefano Maselli

Il Dirigente scolastico
Dott.ssa Chiara De Ioanna