I.I.S. ALESSANDRINI MAINARDI

DOCUMENTO DI E-POLICY

ANNO SCOLASTICO 2020-2021

Parte 1 – INTRODUZIONE

PERCHE' IL DOCUMENTO DI E-POLICY

- I NOSTRI ADOLESCENTI, IPERCONNESSI MA IPERFRAGILI

Fonte:Osservatorio Nazionale Adolescenza

Il 98% dei ragazzi tra i 14 e 1 19 anni ha uno smartphone dai 10 anni di età,il 50% degli adolescenti dichiara di trascorrere dalle 3 alle 6 ore extrascolastiche con lo smartphone in mano, il 16% dalle 7 alle 10 ore,il 10% supera abbondantemente le 10 ore. Il 95% degli adolescenti ha almeno un profilo sui social network e il 14% ne ha uno finto. E' provato che troppo tempo su chat e social aumenta il deficit attentivo e rende facili ala distrazione (alla guida, mentre si passeggia ma anche quando si segue un programma televisivo, si legge un testo, si ascolta …). La dipendenza digitale è una minaccia per la salute mentale dei giovani. Una ricerca pubblicata sulla rivista "Jama pediatrics" svolta nell'arco di 6 anni su ragazze e ragazzi di 12 anni dal 2012 al 2018,ha riportato una stretta correlazione tra ore passate su tv, smartphone e pc e il peggioramento del benessere emotivo e psicologico, peggioramento evidenziato da senso di intorpidimento, irritabilità, calo dell'autostima...L'utilizzo troppo frequente di questi dispositivi è la causa principale di una nuova forma di insonnia che colpisce specialmente gli under 18. Anche la nomofobia, eccessiva paura di rimanere senza smartphone o senza connessione, coinvolge ormai 8 adolescenti su 10. Cresce il gaming disorder, la dipendenza dai videogiochi che in casi estremi può degenerare in forme di violenza. Crescono le proposte online di sfide o giochi, ad esempio il neknominate, social game alcolico che consiste nel creare "catene alcoliche"; la truffa che propone facili guadagni spogliandosi e postando online foto/video: anche siti ritenuti sicuri come Messenger hanno applicazioni come Chatible che permette di chattare con sconosciuti in ogni parte del mondo in modo del tutto anonimo.

I ragazzi usano la Rete quotidianamente, talvolta in modo più "intuitivo" ed "agile" rispetto agli adulti, ma non per questo sono dotati di maggiori "competenze digitali". Infatti, "la competenza digitale presuppone l'interesse per le tecnologie digitali e il loro utilizzo con dimestichezza e spirito critico e responsabile per apprendere, lavorare e partecipare alla società. Essa comprende l'alfabetizzazione informatica e digitale, la comunicazione e la collaborazione, l'alfabetizzazione mediatica, la creazione di contenuti digitali (inclusa la programmazione), la sicurezza (compreso l'essere a proprio agio nel mondo digitale e possedere competenze relative alla cybersicurezza), le questioni legate alla proprietà intellettuale, la risoluzione di problemi e il pensiero critico**" (<u>"Raccomandazione del Consiglio europeo relativa alla competenze chiave per l'apprendimento permanente"</u>, C189/9, p.9).**

PER QUESTO LA SCUOLA SI IMPEGNA A PORTARE AVANTI PERCORSI VOLTI A PROMUOVERE TALI COMPETENZE, AL FINE DI EDUCARE GLI STUDENTI E LE STUDENTESSE VERSO UN USO CONSAPEVOLE E RESPONSABILE DELLE TECNOLOGIE DIGITALI.

- LA PROTEZIONE DEI DATI E LA TUTELA DELLA PRIVACY

La protezione dei dati personali è un diritto fondamentale dell'individuo ai sensi della Carta dei diritti fondamentali dell'Unione europea (art. 8), tutelato dal Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 (relativo alla protezione delle persone

fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati).
Anche le scuole, quindi, hanno oggi l'obbligo di adeguarsi al cosiddetto GDPR (General Data Protection Regulation) e al D.Lgs. 10 agosto 2018, n. 101.
Ogni giorno a scuola vengono trattati numerosi dati personali sugli studenti e sulle loro famiglie. Talvolta tali dati possono riguardare informazioni sensibili, come problemi sanitari o particolari disagi sociali. Il "corretto trattamento dei dati personali" a scuola è condizione necessaria per il rispetto della dignità delle persone, della loro identità e del loro diritto alla riservatezza.
"Le scuole sono chiamate ogni giorno ad affrontare la sfida più difficile, quella di educare le nuove generazioni non solo alla conoscenza di nozioni basilari e alla trasmissione del sapere, ma soprattutto al rispetto dei valori fondanti di una società. Nell'era di Internet e in presenza di nuove forme di comunicazione questo compito diventa ancora più cruciale. È IMPORTANTE RIAFFERMARE QUOTIDIANAMENTE, ANCHE IN AMBITO SCOLASTICO, QUEI PRINCIPI DI CIVILTÀ, COME LA RISERVATEZZA E LA DIGNITÀ DELLA PERSONA, CHE DEVONO SEMPRE ESSERE AL CENTRO DELLA FORMAZIONE DI OGNI CITTADINO".
(cfr. http://www.garanteprivacy.it/scuola).

- LE NUOVE TECNOLOGIE NELLA DIDATTICA

Le TIC (Tecnologie dell'informazione e della comunicazione) rappresentano strumenti fondamentali nel processo educativo e per l'apprendimento degli studenti e delle studentesse. L'emergenza COVID-19 ha messo in luce quanto queste tecnologie possano essere di supporto alla didattica, al limite anche sostituendosi alle metodologie didattiche tradizionali.

Le "competenze digitali" sono fra le abilità chiave all'interno del Quadro di riferimento Europeo delle Competenze per l'apprendimento permanente e di esse bisogna dotarsi proprio a partire dalla scuola (Raccomandazione del Consiglio Europeo del 2006 aggiornata al 22 maggio 2018, relativa alle competenze chiave per l'apprendimento permanente).

- IL DOCUMENTO DI E-POLICY

L'E-policy ha l'obiettivo di esprimere la nostra visione educativa e proposta formativa per garantire il benessere in Rete, definendo le regole di utilizzo delle TIC e ponendo le basi per azioni formative e educative su e con le tecnologie digitali, oltre che di sensibilizzazione su un uso consapevole delle stesse.

Nello specifico:

- l'approccio educativo alle tematiche connesse alle "competenze digitali", alla privacy, alla sicurezza online e all'uso delle tecnologie digitali nella didattica e nel percorso educativo;
- le norme comportamentali e le procedure di utilizzo delle Tecnologie dell'Informazione e della Comunicazione (ICT) in ambiente scolastico;
- le misure per la prevenzione e la sensibilizzazione di comportamenti on-line a rischio;
- le misure per la rilevazione, segnalazione e gestione delle situazioni rischiose legate ad un uso non corretto delle tecnologie digitali.

Parte 2-ARGOMENTI DEL DOCUMENTO

- Presentazione dell'e-Policy
  - Scopo dell'e-Policy
  - Ruoli e responsabilità
  - Un'informativa per i soggetti esterni che erogano attività educative nell'Istituto
  - Condivisione e comunicazione dell'e-Policy all'intera comunità scolastica
  - Gestione delle infrazioni alla e-Policy
  - Integrazione dell'e-Policy con regolamenti esistenti
  - Monitoraggio dell'implementazione dell'e-Policy e suo aggiornamento
- Formazione e curricolo
  - Curricolo sulle competenze digitali per gli studenti
  - Formazione dei docenti sull'utilizzo e l'integrazione delle TIC (Tecnologie dell'Informazione e della Comunicazione) nella didattica e sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali
  - Sensibilizzazione delle famiglie e Patto di corresponsabilità
- Gestione dell'infrastruttura e della strumentazione ICT (Information and Communication Technology) della e nella scuola
  - Protezione dei dati personali
  - Accesso ad Internet
  - Strumenti di comunicazione online,strumentazione personale, regolamentazione d'uso
- Rischi on line: conoscere, prevenire e rilevare
  - Sensibilizzazione e prevenzione. Il progetto dell'Istituto
- Segnalazione e gestione dei casi
  - Cosa segnalare
  - Come segnalare: quali strumenti e a chi
  - Gli attori sul territorio per intervenire
  - Allegati con le procedure

Parte 3 – DOCUMENTO DI E-POLICY

- SCOPO DELL'E-POLICY

La **E-policy** è un documento programmatico volto a promuovere le competenze digitali ed un uso delle tecnologie positivo, critico e consapevole, sia da parte dei ragazzi e delle ragazze che degli adulti coinvolti nel processo educativo. Inoltre, vuole essere un documento finalizzato sviluppare, attraverso specifiche azioni, una conoscenza delle opportunità e dei rischi connessi all'uso di Internet, quindi a prevenire situazioni problematiche e a riconoscere, gestire, segnalare e monitorare episodi legati ad un utilizzo scorretto degli strumenti.

- RUOLI E RESPONSABILITA' NELLA E-POLICY

Affinché l'E-policy sia davvero uno strumento operativo efficace per la scuola e tutta la comunità educante è necessario che ognuno, secondo il proprio ruolo, s'impegni nell'attuazione e promozione di essa.

Per quanto riguarda la corresponsabilità educativa si ricorda che esistono tre tipi di "reati" :culpa in vigilando, imputabile al docente, culpa in organizzando imputabile al DS, e culpa in educando imputabile ai genitori. Quindi tutti i soggetti sono tenuti ad essere informati sui contenuti del documento , a cui verrà data la massima diffusione.

Ruolo	Responsabilità
DIRIGENTE SCOLASTICO	-è il responsabile della sicurezza dei dati -è il garante dell'applicazione della e-policy -individua referente per il bullismo e cyber bullismo - si impegna a garantire a tutti i docenti ed alunni, soprattutto quelli in entrata, la formazione per l'uso responsabile e corretto delle Tecnologie dell'Informazione e della comunicazione (alcune ore di lezione all'anno sulla websecurity nelle TIC), oltre che nell'uso personale, anche nella didattica, in collaborazione con il team digitale -si impegna a dotare la scuola di un sistema in grado di consentire il controllo della sicurezza in rete -si impegna a seguire le procedure relative agli eventi dannosi eventualmente occorsi agli alunni nell'utilizzo delle TIC a scuola.
ANIMATORE DIGITALE	-promuove la formazione interna in ambito tecnologico-digitale oltre che a fungere da referente per ogni informazione riguardo i rischi della rete, le relative misure di prevenzione nonché la gestione operativa delle eventuali problematiche -rileva e/o raccoglie le criticità proponendo soluzioni adeguate e sostenibili - si interessa dell'aggiornamento delle politiche di istituto sulla sicurezza della rete della scuola, e della proposta di novità ed

	aggiornamento metodologico e tecnologico implementabile nella rete di istituto ad uso di tutto il personale scolastico; - si impegna a gestire e controllare l'accesso alla rete ed ai servizi di istituto (posta elettronica,Gsuite,ecc.) da parte degli utenti mediante credenziali personalizzate, firewall, antivirus, ecc. -individua in collaborazione con le figure di sistema e il referente del bullismo e cyberbullismo progetti ed attività aventi ad oggetto la sicurezza in rete in cui coinvolgere la comunità scolastica .
REFERENTE CYBERBULLISMO	-promuove attività, eventi funzionali alla prevenzione delle problematiche inerenti al cyber bullismo e al tema della sicurezza in Rete.
DSGA	-assicura, nei limiti delle risorse finanziarie, la manutenzione delle strutture informatiche ai fini del suo funzionamento, della sua sicurezza e tutela da un uso improprio, e da attacchi esterni -garantisce la comunicazione all'interno dell'istituto, (sportello, circolari, sito web, ecc.), e tra le reti di scuole e fra la scuola e le famiglie degli alunni per la diffusione di informazioni nell'ambito dell'utilizzo delle tecnologie digitali e della rete.
DOCENTI	Hanno il compito di -informarsi ed aggiornarsi su tema della sicurezza in rete uniformandosi alle politiche di sicurezza adottate dalla scuola di cui rispettano il regolamento - integrare nel curriculum di studio e nelle attività didattiche ed educative delle classi le modalità di utilizzo corretto e sicuro delle TIC e di Internet -specialmente ora che è necessario avvalersi della DDI e della DAD a causa dell'emergenza Covid-19 - assicurandosi che gli alunni abbiano una buona comprensione delle opportunità di ricerca offerte dalle tecnologie digitali e dalla rete ma anche della necessità di evitare il plagio e di rispettare la normativa sul diritto d'autore. Sarà data particolare attenzione nell'educazione sulla sicurezza agli aspetti per i quali gli alunni risultano più esposti o rispetto ai quali risultano più vulnerabili - supportare gli alunni nel corretto utilizzo delle tecnologie digitali per finalità didattico-educative (controllo nel rispetto delle leggi, del regolamento interno, del plagio, del diritto d'autore, ecc), guidandoli nella scelta delle fonti di informazione -garantire che le comunicazioni con i mezzi informatici avvengano nel rispetto dei ruoli e dei rispettivi codici comportamentali, mediante canali ufficiali e verificabili (posta elettronica col dominio dell'istituto, G-suite, ecc.) -rispettare l'obbligo di riservatezza dei dati personali trattati e

	non, in conformità alla normativa vigente - interagire con i genitori, coordinando con gli stessi l'intervento educativo, nei casi di disagio, manifestato dall'alunno, collegato all'utilizzo delle tecnologie digitali -segnalare all'Animatore digitale eventuali criticità nei sistemi informativi soprattutto in materia di prevenzione e gestione dei rischi nell'uso delle TIC -seguire le procedure interne di segnalazione di eventuali abusi subiti dagli alunni e connessi all'uso delle tecnologie digitali
ALUNNI	Devono imparare a: -utilizzare responsabilmente le tecnologie digitali uniformandosi alle indicazioni dei docenti nonché rispettando le norme codificate nei regolamenti di istituto -rispettare le buone pratiche di sicurezza in rete -saper distinguere, con l'aiuto dei docenti, le fonti di informazione attendibili in rete per utilizzarle in modo appropriato senza violazione dei diritti d'autore altrui; - comunicare in rete in modo appropriato rispettando le posizioni altrui -segnalare ai genitori e/o ai docenti situazioni di difficoltà o di bisogno di aiuto nell'utilizzo delle tecnologie digitali -segnalare a docenti e/o genitori casi di abuso nell'utilizzo dei social a scuola
GENITORI	Hanno il compito di: -sostenere i docenti nell'azione educativa diretta al corretto utilizzo delle tecnologie digitali - educare, vigilando sui propri figli, al corretto utilizzo delle tecnologie digitali in ambiente domestico fissando regole comportamentali e di utilizzo -collaborare con i docenti nell'adozione di linee di intervento coerenti per contrastare l'uso non responsabile, scorretto o pericoloso delle tecnologie digita
PERSONALE A.T.A.	-è tenuto a conoscere e mettere in pratica i regolamenti redatti dall'Istituto - a segnalare tempestivamente eventuali violazioni. -a partecipare alle attività di formazione proposte in istituto

- SOGGETTI ESTERNI CHE EROGANO ATTIVITA' EDUCATIVE ALL'INTERNO DELL'ISTITUTO

Ogni volta che ci si avvale di soggetti esterni per ampliare l'offerta formativa dell'Istituto è bene che siano informati sui contenuti essenziali del documento di e-policy per quanto riguarda l'insieme di regole e di norme di comportamento da seguire e le procedure di segnalazione nel caso si rilevino infrazioni. Essi sono tenuti a conoscere e rispettare le regole del nostro Istituto dove sono esplicitate le modalità di utilizzo dei propri dispositivi personali (smartphone, tablet, pc, etc.) e quelli in dotazione della scuola, evitando un uso improprio o comunque deontologicamente scorretto durante le attività con gli studenti e le studentesse. Esiste l'obbligo di rispettare la privacy, soprattutto dei soggetti minorenni, in termini di fotografie, immagini, video o scambio di contatti personali (numero, mail, chat, profili di social network).

A chi, in qualità di soggetto esterno, farà attività all'interno dell'istituto verrà data una sintesi del documento di e-policy e una copia del modulo per le segnalazioni.

- INTEGRAZIONE DELLA E-POLICY CON I REGOLAMENTI ESISTENTI E

CONDIVISIONE E COMUNICAZIONE ALL'INTERA COMUNITA' SCOLASTICA

Il documento di E-policy, dopo l'approvazione del Collegio dei Docenti e dal Consiglio di Istituto , verrà pubblicato sul sito istituzionale della scuola ed esposto in versione semplificata negli spazi che dispongono di pc collegati alla Rete e all'ingresso dell'Istituto.

Inoltre un suo estratto verrà inserito nel Regolamento di Istituto e nel Patto di Corresponsabilità, che deve essere sottoscritto dalle famiglie e rilasciato alle stesse all'inizio dell'anno scolastico.

Gli studenti e le studentesse vengono informati sul fatto che sono monitorati e supportati nella navigazione online, negli spazi della scuola e sulle regole di condotta da tenere in Rete.

L'elenco delle regole per la sicurezza on-line sarà sul sito.

Tutto il personale scolastico, gli alunni e i genitori saranno informati che la rete, l'uso di Internet e di ogni dispositivo digitale saranno controllati dagli insegnanti e utilizzati solo con la loro autorizzazione.

Si potrà fare riferimento all' Animatore digitale perché siano messi a disposizione utili strumenti da usare con gli alunni in classe.
In particolare tutto il personale dovrà essere consapevole che:
- il traffico in internet può essere monitorato e si potrà risalire al singolo utente registrato. Il Dirigente scolastico può controllare l'utilizzo delle TIC per verificarne la conformità alle regole di sicurezza, compreso l'accesso a internet,la posta elettronica inviata/pervenuta a scuola, procedere alla cancellazione di materiali inadeguati o non autorizzati dal sistema informatico della scuola,conservandone una copia per eventuali successive investigazioni.
- una condotta non in linea con il codice di comportamento dei pubblici dipendenti e i propri doveri professionali è sanzionabile.

Le procedure sono quelle previste dalla legge e dai contratti di lavoro.

Per impedire che le stesse postazioni dei laboratori scolastici possano essere utilizzate per visitare siti volgari e pericolosi, la scuola si è da tempo dotata di un software di sicurezza che filtra gli accessi ad internet e protegge quindi i visitatori meno esperti.
Oltre a questo sistema di protezione la scuola ovviamente mette in campo soprattutto la vigile attenzione educativa di ogni singolo docente.
La scuola non pone alcun ostacolo all'utilizzo di cd/dvd rom o di hard - disk portatili come strumenti di lavoro e di studio. Ciò che a riguardo compete alle famiglie è il controllo periodico del contenuto di questi strumenti per evitare che qualche studente 'trasporti' a scuola immagini / testi /filmati inappropriati avendoli scaricati altrove.

- GESTIONE DELLE INFRAZIONE ALLA E-POLICY

La scuola gestirà le infrazioni all'E-policy attraverso azioni educative e/o sanzioni, qualora fossero necessarie, valutando i diversi gradi di gravità di eventuali violazioni.

le infrazioni più comuni in cui possono incorrere gli **studenti** sono:
-un uso della rete per giudicare, infastidire o impedire a qualcuno di esprimersi o partecipare;
-l'invio incauto o senza permesso di foto o di altri dati personali come l'indirizzo di casa o il telefono;
-la condivisione di immagini intime o troppo spinte;
-la comunicazione incauta e senza permesso con sconosciuti;
-il collegamento a siti web non indicati dai docenti.
I possibili provvedimenti "disciplinari",proporzionati alla gravità del comportamento sono già riportati nel Regolamento di Disciplina.

In particolare se si concretizzano durante l'orario scolastico episodi che si possono configurare come reati non si esclude la segnalazione ai competenti organi di Pubblica Sicurezza.
Contestualmente sono previsti interventi di carattere educativo, anche attraverso l'intervento della psicopedagogista, di rinforzo dei comportamenti corretti e riparativi dei disagi causati,di ri-definizione delle regole sociali di convivenza attraverso la partecipazione consapevole e attiva degli alunni della classe, di prevenzione e gestione positiva dei conflitti, di moderazione dell'eccessiva competitività, di promozione di rapporti amicali e di reti di solidarietà, di promozione della conoscenza e della gestione delle emozioni.
Anche alcune condizioni e condotte dei genitori possono favorire o meno l'uso corretto e responsabile delle TIC da parte degli alunni a scuola, in particolare una piena autonomia concessa al proprio figlio nella navigazione sul web e nell'utilizzo del cellulare o dello smartphone. Da qui l'importanza di coinvolgere i genitori in base alla gravità dei comportamenti dei loro figli,se dovessero risultare pericolosi per sé e/o dannosi per gli altri.

- MONITORAGGIO DELL'IMPLEMENTAZIONE DELLA E-POLICY E SUO AGGIORNAMENTO

L'E-policy viene aggiornata periodicamente e quando si verificano cambiamenti significativi in riferimento all'uso delle tecnologie digitali all'interno della scuola, per esempio in relazione alle attività in DAD o in modalità blended previste a causa dell'emergenza COVID-19. In merito si fa riferimento al Regolamento di Istituto , al Patto di corresponsabilità e al Regolamento di

disciplina reperibili sul sito istituzionale. Il monitoraggio del documento sarà realizzato a partire da una valutazione della sua efficacia in riferimento agli obiettivi specifici che lo stesso si pone.

Parte 4 - FORMAZIONE E CURRICOLO

- CURRICOLO SULLE COMPETENZE DIGITALI PER GLI STUDENTI

Vista la peculiarità del nostro istituto, che prevede nel curricolo le discipline di Informatica ed Elettronica, la formazione degli studenti rientra nel curriculo del biennio e sarà portata avanti dai docenti in servizio anche laddove non sono previste le materie specifiche. In particolare gli studenti riceveranno una formazione specifica riguardo all'utilizzo dei devices di uso quotidiano, con attenzione alle problematiche che ne derivano dall'uso improprio.

- FORMAZIONE DEI DOCENTI E DEL PERSONALE SCOLASTICO SULL'UTILIZZO E L'INTEGRAZIONE DELLE TIC (TECNOLOGIE DELL'INFORMAZIONE E DELLA COMUNICAZIONE) NELLA DIDATTICA E SULL'UTILIZZO CONSAPEVOLE E SICURO DI INTERNET E DELLE TECNOLOGIE DIGITALI

La scuola si impegna a promuovere specifici momenti di aggiornamento che, con cadenza, verranno organizzati dall'Istituto scolastico con la collaborazione del personale specializzato interno e se necessario del personale esterno e con il supporto della rete scolastica del territorio delle amministrazioni comunali, dei servizi socio-educativi e delle associazioni presenti. In particolare gli argomenti su cui verranno proposti momenti periodici di aggiornamento sono:

-utilizzo degli strumenti nella ddi

-metodologie didattiche per la ddi

-formazione gestione privacy (gdpr) anche per il personale ATA

Altre attività di aggiornamento scaturiranno dall'analisi del fabbisogno formativo di docenti e studenti.

- SENSIBILIZZAZIONE FAMIGLIE E PATTO DI CORRESPONSABILITA'

Il documento di e-policy è visionabile sul sito dell'Istituto. All'atto dell'iscrizione i genitori, per le studentesse e gli studenti minorenni, ricevono copia del patto di Corresponsabilità da restituire firmato. Qualora se ne dovesse manifestare la necessità saranno previsti incontri di informazione/formazione anche per i genitori.

Parte 5 - GESTIONE DELL'INFRASTRUTTURA E DELLA STRUMENTAZIONE ICT (INFORMATION AND COMMUNICATION TECHNOLOGY) DELLA E NELLA SCUOLA

- PROTEZIONE DEI DATI PERSONALI

L'istituto ha scelto di utilizzare per la DAD la piattaforma G-Suite di Google e la mette a disposizione dei propri studenti e insegnanti promuovendo una didattica cooperativa, laboratoriale e per competenze, che educhi ad un utilizzo responsabile della tecnologia, come previsto dal PNSD, abituando contemporaneamente gli alunni a collaborare, anche a distanza. Ogni docente ha un account attraverso il quale usare varie applicazioni Google, come strumenti didattici utilizzando una modalità professionale e professionalizzante.
Le norme tecniche relative all'uso dei servizi della Google Suite sono reperibili sul seguente sito: https://gsuite.google.it/learning-center/.
Contemporaneamente ogni utente potrà anche consultare le privacy policy di Google sul sito.
Per quanto riguarda la gestione del proprio account personale da parte di studentesse e studenti valgono le seguenti regole generali. L'utente:

-è responsabile delle azioni compiute tramite il suo account e, pertanto, esonera l'Istituto da ogni pretesa o azione che dovesse essere rivolta all'Istituto medesimo da qualunque soggetto, in conseguenza di un uso improprio.

- si impegna a non diffondere eventuali informazioni riservate di cui venisse a conoscenza, relative all'attività delle altre persone che utilizzano il servizio;

-prende atto che è vietato servirsi o dar modo ad altri di servirsi del servizio di posta elettronica e delle applicazioni Google messe a disposizione dall'Istituto per danneggiare, violare o tentare di violare il segreto della corrispondenza e il diritto alla riservatezza.

-si impegna a non trasmettere o condividere informazioni che possano presentare forme o contenuti di carattere pornografico, osceno, blasfemo, diffamatorio o contrario all'ordine pubblico o alle leggi in materia civile, penale ed amministrativa vigenti.

-nel caso in cui utilizzi la strumentazione digitale dell'Istituto, ha il dovere di disconnettersi dal proprio account, una volta terminata l'attività; questo per evitare spiacevoli occasioni di violazione della privacy. La password personale non va pertanto memorizzata sui dispositivi non personali.

- ACCESSO AD INTERNET

Il diritto di accesso a Internet è presente nell'ordinamento italiano - 'art. 2 della Dichiarazione dei diritti di Internet(2014) presso la Camera dei Deputati - ed europeo - il Regolamento UE del Parlamento Europeo (2016) -e la scuola dovrebbe essere il luogo dove tale diritto è garantito, anche per quegli studenti che non dispongono della Rete a casa. In modo coerente il PNSD (Piano Nazionale Scuola Digitale) ha tra gli obiettivi quello di "fornire a tutte le scuole le condizioni per l'accesso alla società dell'informazione e fare in modo che il "diritto a Internet" diventi una realtà, a partire dalla scuola".
Questo perché le tecnologie da un lato contribuiscono a creare un ambiente che può rendere la scuola aperta, flessibile e inclusiva, dall'altro le consentono di adeguarsi ai cambiamenti della società e del mercato del lavoro, puntando a sviluppare una cultura digitale diffusa che deve iniziare proprio a scuola. Quindi per legge

- L’accesso a Internet è diritto fondamentale della persona e condizione per il suo pieno sviluppo individuale e sociale.
- Ogni persona ha eguale diritto di accedere a Internet in condizioni di parità, con modalità tecnologicamente adeguate e aggiornate che rimuovano ogni ostacolo di ordine economico e sociale.
- Il diritto fondamentale di accesso a Internet deve essere assicurato nei suoi presupposti sostanziali e non solo come possibilità di collegamento alla Rete.
- L'accesso comprende la libertà di scelta per quanto riguarda dispositivi, sistemi operativi e applicazioni anche distribuite.
- L’Istituto, in qualità di Istituzione Pubblica, garantisce i necessari interventi per il superamento di ogni forma di divario digitale tra cui quelli determinati dal genere, dalle condizioni economiche oltre che da situazioni di vulnerabilità personale e disabilità.

- STRUMENTI DI COMUNICAZIONE ONLINE - STRUMENTAZIONE PERSONALE REGOLE PER USO DEI CELLULARI, DELLE APPARECCHIATURE ELETTRONICHE REGOLE PER L’UTILIZZO DEI SOCIAL NETWORK

Le tecnologie digitali sono in grado di ridefinire gli ambienti di apprendimento, supportando la comunicazione a scuola e facilitando un approccio sempre più collaborativo. L’uso degli strumenti di comunicazione online a scuola, al fianco di quelli più tradizionali, ha l’obiettivo di rendere lo scambio comunicativo maggiormente interattivo e orizzontale. Tale uso segue obiettivi e regole precise correlati alle caratteristiche, funzionalità e potenzialità delle tecnologie digitali.
I dispositivi tecnologici sono parte integrante della vita personale di ciascuno, compresa quella di studentesse e studenti e dei docenti,oltre che di tutte le figure professionali che a vario titolo sono inseriti nel mondo della scuola, ed influenzano necessariamente anche la didattica e gli stili di apprendimento. E’ necessario però disciplinarne l’uso in classe anche in considerazione dei dieci punti del Miur per l’uso dei dispositivi mobili a scuola (BYOD, “Bring your own device”).

In tutta l’area scolastica è tassativamente vietato registrare immagini, sia statiche (fotografie), sia dinamiche (videofilmati), voci o suoni senza preventiva autorizzazione della Presidenza (tali azioni si configurano come gravi violazioni dell’immagine e della privacy secondo il D.L. 30/06/2003).
E’ altresì vietato agli studenti l’uso in classe dei telefoni cellulari e di qualsiasi altra apparecchiatura tecnologica senza preventiva autorizzazione dell’insegnante.
Se durante i compiti in classe lo studente viene trovato in possesso del cellulare acceso, l’insegnante può ritirare il compito e valutarlo negativamente.

In classe l’utilizzo dei social network è consentito solo per esigenze didattiche e solo se autorizzato dall’insegnante.
Le seguenti azioni, che prevedono l’utilizzo dei social network per intenti illeciti, sono considerate reati e, in alcuni casi, sono sanzionabili d'ufficio, anche in assenza di una denuncia da parte dell'interessato:
• Invio di materiale pubblicitario non autorizzato (spamming)
• Raccolta e utilizzo indebito di dati personali, (attività già espressamente vietate

dal T.U. sulla privacy ,d.lgs. n. 196 del 2003)
• Utilizzo dei contatti per trasmettere volutamente virus informatici (c.p. art. 615)
• Utilizzo dei contatti per acquisire abusivamente codici di accesso per violare sistemi informatici (c.p. art. 615)
• Produzione, commercio, distribuzione, divulgazione e cessione di materiale pornografico coinvolgente minori (c.p. art. 600): "
• Detenzione di materiale pornografico prodotto mediante lo sfruttamento sessuale dei minori (c.p. Art. 600)
• Invio di messaggi di propaganda politica, di incitamento all'odio e di discriminazione razziale
• Inserimento di frasi offensive o battute pesanti, notizie riservate la cui divulgazione provoca pregiudizi, foto denigratorie o comunque la cui pubblicazione ha ripercussioni negative, anche potenziali, sulla reputazione della persona ritratta. Tale reato è punito dall'art. 595 c.p. fino a 3 anni di reclusione (nelle forme aggravate), con annesso diritto al risarcimento nei confronti della parte lesa.
• Sostituzione di persona e usurpazione di titoli e onori. E' considerato reato il comportamento di chi crea un falso account di posta elettronica, intrattenendo corrispondenze informatiche con altre.
• Offese a una confessione religiosa.

Parte 6 - RISCHI ONLINE

Il rischio online si configura come la possibilità per il minore di:

- commettere azioni online che possano danneggiare se stessi o altri;
- essere una vittima di queste azioni;
- osservare altri commettere queste azioni.

La posizione dell' Istituto è quella di intervenire con attività che possano permettere una riduzione dei fattori di rischio e di conseguenze una minore probabilità che i ragazzi si trovino in situazioni non piacevoli. È importante che abbiano gli strumenti idonei per riconoscere possibili situazioni di rischio e segnalarle ad un adulto di riferimento. I progetti in essere lavorano sia sul piano della sensibilizzazione che su quello della prevenzione.

- CYBERBULLISMO

La legge 71/2017 "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo", nell'art. 1, comma 2, definisce il cyberbullismo:

"qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali in danno di minorenni, realizzata per via telematica, nonché la

diffusione di contenuti on line aventi ad oggetto anche uno o più componenti della famiglia del minore il cui scopo intenzionale e predominante sia quello di isolare un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo".

La nostra scuola è sempre stata sensibile nei confronti di queste tematiche e quindi, a partire dall'a.s. 2016-2017, ha provveduto a:

- formare il personale scolastico, prevedendo la partecipazione di un proprio referente per ogni autonomia scolastica;
- favorire lo sviluppo delle competenze digitali
- promozione di un ruolo attivo degli studenti in attività di peer education;
- fornire agli studenti gli strumenti necessari per decostruire gli stereotipi su cui spesso si fondano forme di cyberbullismo, in particolare legati alla razza, al genere, all'orientamento sessuale, alla disabilità;
- promuovere la partecipazione civica e l'impegno, anche attraverso i media digitali e i social network;
- favorire una presa di parola consapevole e costruttiva da parte dei giovani;
- previsione di misure di sostegno e rieducazione dei minori coinvolti, avvalendosi della collaborazione di una psicopedagogista, esperta nella trattazione dei problemi dell'età evolutiva
- Integrazione dei regolamenti e del patto di corresponsabilità con specifici riferimenti a condotte di cyberbullismo e relative sanzioni disciplinari commisurate alla gravità degli atti compiuti.

Come da legge del 23 /07/2018 è stato nominato un docente referente per le iniziative di prevenzione e contrasto che:

- Ha il compito di coordinare le iniziative di prevenzione e contrasto del cyberbullismo. A tal fine, può avvalersi della collaborazione delle Forze di polizia e delle associazioni e dei centri di aggregazione giovanile del territorio.
- Potrà svolgere un importante compito di supporto al dirigente scolastico per la revisione/stesura di Regolamenti (Regolamento d'istituto), atti e documenti (PTOF, PdM, Rav).

Per quanto riguarda il bullismo e il cyber bullismo il link seguente riporta a quanto pubblicato sul sito dell'Istituto a cura del docente referente

https://www.alessandrinimainardi.edu.it/sites/default/files/page/2019/bullismo-e-cyberbullismo.pdf

In particolare è attivo dall'a.s. 2016-2017 un progetto di sensibilizzazione e prevenzione denominato "io non casco nella Rete", che viene proposto alle classi prime e seconde, pubblicato sul sito dell'istituto.

https://www.alessandrinimainardi.edu.it/sites/default/files/page/2018/il-progetto-io-non-casco-nella-rete.pdf

Nel progetto sono previste diverse azioni:
-la sensibilizzazione verso il tema del bullismo e del cyber bullismo (classi prime)
-la trattazione, con lo strumento della peer education, dei principali pericoli in cui un adolescente può imbattersi navigando in Rete senza adeguati strumenti
- la sensibilizzazione verso il tema della "hate speech" (classi seconde).

Parte 7 – SEGNALAZIONE E GESTIONE DEI CASI

- COSA SEGNALARE

Il personale docente e non docente e gli alunni stessi devono avviare una segnalazione quando hanno il sospetto o la certezza che UNA STUDENTESSA O UNO STUDENTE possa essere vittima o responsabile
-di una situazione di cyber bullismo o reati connessi (adescamento, hate speech…)
-della violazione delle regole che riguardano l'utilizzo di Internet e dei social network.

- COME E A CHI SEGNALARE

Questa sezione dell'e-Policy contiene le procedure standardizzate per la segnalazione e gestione dei problemi connessi a comportamenti online a rischio di studenti e studentesse (vedi allegati a seguire).
Tali procedure dovranno essere una guida costante per gli alunni , il personale della scuola ed anche per i professionisti e le organizzazioni esterne che collaborano con l'Istituto.

Si ricorda che L'insegnante riveste la qualifica di pubblico ufficiale in quanto l'esercizio delle sue funzioni non è circoscritto all'ambito dell'apprendimento, ossia alla sola preparazione e tenuta delle lezioni, alla verifica/valutazione dei contenuti appresi dagli studenti e dalle studentesse, ma si estende a tutte le altre attività educative. Quindi ha anche il compito di gestire le situazioni problematiche in relazione all'uso delle tecnologie digitali, sia che si tratti di un caso sospetto oppure di un'evidenza.
Nell'affrontare i casi prevediamo la collaborazione con figure esterne, nella fattispecie una psicopedagogista,qualora la gravità e la sistematicità della situazione richieda interventi che esulano dalle competenze e possibilità della scuola.

Nelle procedure:
- sono indicate le figure preposte all'accoglienza della segnalazione e alla presa in carico e gestione del caso.
- le modalità di coinvolgimento del referente per il contrasto del bullismo e del cyberbullismo, oltre al Dirigente Scolastico.

Per quanto riguarda la necessità di segnalazione e rimozione di contenuti online lesivi, ciascun minore ultraquattordicenne (o i suoi genitori o chi esercita la responsabilità del minore) che sia stato vittima di cyberbullismo può inoltrare al titolare del trattamento o al gestore del sito internet o del social media un'istanza per l'oscuramento, la rimozione o il blocco dei contenuti diffusi nella Rete. Se entro 24 ore il gestore non avrà provveduto, l'interessato può rivolgere

analoga richiesta al Garante per la protezione dei dati personali, che rimuoverà i contenuti entro 48 ore.
Sono attivi inoltre i seguenti servizi:
- Servizio di Helpline 19696 e Chat di Telefono Azzurro per supporto ed emergenze;
- Clicca e segnala di Telefono Azzurro e STOP-IT di Save the Children Italia per segnalare la presenza di materiale pedopornografico online.

Le procedure sono condivise attraverso il sito dell'Istituto e nelle assemblee scolastiche che coinvolgono i genitori, studentesse e studenti. Sono affisse alla bacheca di Istituto perché ne possa prendere visione tutto il personale scolastico.

Allegati con le procedure.

Strumenti a disposizione di studenti/esse

Per aiutare studenti/esse a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni, la scuola prevede alcuni strumenti di segnalazione ad hoc messi a loro disposizione:

- un indirizzo e-mail specifico per le segnalazioni;
- scatola/box per la raccolta di segnalazioni anonime da inserire in uno spazio accessibile e ben visibile della scuola;
- sportello di ascolto con professionisti;
- docente referente per le segnalazioni.

Anche studenti e studentesse, inoltre, possono rivolgersi alla Helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96.
DOBBIAMO DECIDERE COSA UTILIZZARE

- GLI ATTORI SUL TERRITORIO

Qualora nella gestione dei casi può essere necessario rivolgersi ad altre figure, enti, istituzioni e servizi presenti sul territorio , perché la gravità e la sistematicità della situazione richieda interventi che esulano dalle competenze e possibilità della scuola,
segue un elenco degli indirizzi di strutture che è possibile consultare
A seguire i principali Servizi e le Agenzie deputate alla presa in carico dei vari aspetti che una problematica connessa all'utilizzo di Internet può presentare.

- Comitato Regionale Unicef: laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell'infanzia.
- Co.Re.Com. (Comitato Regionale per le Comunicazioni): svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare attenzione alla tutela dei minori.
- Ufficio Scolastico Regionale: supporta le scuole in attività di prevenzione ed anche nella segnalazione di comportamenti a rischio correlati all'uso di Internet.
- Polizia Postale e delle Comunicazioni: accoglie tutte le segnalazioni relative a comportamenti a rischio nell'utilizzo della Rete e che includono gli estremi del reato.
- Aziende Sanitarie Locali: forniscono supporto per le conseguenze a livello psicologico o psichiatrico delle situazioni problematiche vissute in Rete. In alcune regioni, come il Lazio e

la Lombardia, sono attivi degli ambulatori specificatamente rivolti alle dipendenze da Internet e alle situazioni di rischio correlate.

- Garante Regionale per l'Infanzia e l'Adolescenza e Difensore Civico: segnalano all'Autorità Giudiziaria e ai Servizi Sociali competenti; accolgono le segnalazioni di presunti abusi e forniscono informazioni sulle modalità di tutela e di esercizio dei diritti dei minori vittime. Segnalano alle amministrazioni i casi di violazione e i fattori di rischio o di danno dovute a situazioni ambientali carenti o inadeguate.
- Tribunale per i Minorenni: segue tutti i procedimenti che riguardano reati, misure educative, tutela e assistenza in riferimento ai minori.

https://www.generazioniconnesse.it/_file/documenti/E-LEARNING-LEZIONI/Corso-5/Scheda%20di%20segnalazione.docx

seguono allegati

all 1

PROCEDURA DI SEGNALAZIONE E INTERVENTO

AZIONE	PERSONE COINVOLTE	ATTIVITÀ
1) SEGNALAZIONE	• Insegnanti • Personale ATA • Alunni • Genitori	Segnalare presunti episodi di bullismo/cyberbullismo attraverso la compilazione del "**MODULO PER LA SEGNALAZIONE DI EPISODI DI BULLISMO E/O CYBERBULLISMO**". Il modulo può essere inserito nell'apposita scatola predisposta vicino ai centralini nei due ingressi o inviato per mail o consegnato in ufficio protocollo o al Dirigente o al Referente per il Bullismo **NB il Modulo va compilato anche in caso di segnalazione orale.**
2) RACCOLTA INFORMAZIONI	• Referente bullismo e cyber bullismo	Raccogliere, verificare e valutare le informazioni contenute nei moduli di segnalazione.
3) INTERVENTI EDUCATIVI	• Dirigente • Coordinatori di classe • Consiglio di classe • Insegnanti • Alunni • Genitori • Psicologa	• Incontri con gli alunni coinvolti • Interventi/discussione in classe • Informare e coinvolgere i genitori • coinvolti • Ribadire regole di comportamento • Counselling • Incontri formativi con esperti esterni
4) INTERVENTI DISCIPLINARI	• Dirigente • Consiglio di classe	Vedi "Statuto degli studenti e delle studentesse" e Regolamento di disciplina dell'istituto
5) VALUTAZIONE	• Dirigente • Consiglio di classe	Dopo gli interventi educativi e disciplinari, valutare se il problema è stato risolto. Se la situazione continua si proseguire con altri interventi. L'attenzione, l'osservazione e il monitoraggio rimangono in ogni caso costanti.

All 2

Intestazione scuola?

MODULO PER LA SEGNALAZIONE DI EPISODI DI BULLISMO E/O CYBERBULLISMO E REATI CORRELATI ALL'UTILIZZO DEI SOCIAL NETWORK

NOME e COGNOME di chi segnala:	

RUOLO (insegnante, genitore, alunno, ...):	

- Cosa è successo?
  Descrivere l'accaduto: Pressioni - aggressione - molestia - ricatto - ingiuria - denigrazione - diffamazione - furto d'identità *(es: qualcuno finge di essere me sui social network, hanno rubato le mie password e utilizzato il mio account sui social network, ecc.)* - alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali *(es: qualcuno ha ottenuto e diffuso immagini, video o informazioni che mi riguardano senza che io volessi, ecc.)* - diffusione online di dati e informazioni (video, foto, post, ecc.) per attaccare o ridicolizzare me, e/o la mia famiglia e/o il mio gruppo

_____
_____
_____

Altro: specificare

_____
_____
_____

- Quando (specificare se è la prima volta)

  _____

- In quale luogo dell'Istituto?_____

- Dove? (specificare)

Sito internet_____

Social network_____

Altro_____

Se possibile, allegare all'e-mail immagini, video, *screenshot* e/o altri elementi informativi utili relativi all'accaduto

- Elenco delle persone eventualmente presenti al fatto

_____
_____
_____

- Elenco delle persone che sono state informate, a vario titolo, dell'accaduto

_____
_____
_____

Luogo e data_____ firma_____