INDICE RAGIONATO
E-Safety Policy

Introduzione
Scopo della Policy.
Lo scopo della E-Safety Policy è di stabilire i principi fondamentali tipici di tutti i membri della comunità scolastica per quanto riguarda l'utilizzo di tecnologie; salvaguardare e proteggere i bambini, i ragazzi e lo staff dell'Istituto; assistere il personale della scuola a lavorare in modo sicuro e responsabile con altre tecnologie di comunicazione di Internet e monitorare i propri standard e le prassi; 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, che sono riferimenti incrociati con le altre politiche della scuola; 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.

Le principali aree di rischio per la nostra comunità scolastica possono essere riassunte come segue:
Contenuto
- l'esposizione a contenuti inappropriato
- visita di siti web inappropriato
- siti di odio
- validazione dei contenuti: come controllare l'autenticità e l'esattezza dei contenuti online.

Contatto
- grooming
- bullismo online in tutte le forme
- il furto di identità

Condotta
- questioni di privacy, tra cui la divulgazione di informazioni personali
- reputazione online
- la salute e il benessere (quantità di tempo speso online su Internet o giochi)
- sexting (invio e ricezione di immagini personali intime)
- l'estremismo
- il copyright (poca cura o considerazione per i diritti d'autore relativamente a musica e film)

Ruoli e Responsabilità (*che cosa ci si aspetta da tutti gli attori della Comunità Scolastica*).

RUOLO	RESPONSABILITA'
Il 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 online 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.
Il responsabile della sicurezza online (DSGA e docente su nomina del DS)	la responsabilità per i problemi di sicurezza online; promuovere la consapevolezza e l'impegno per la salvaguardia online di tutta la comunità scolastica; assicurare che l'educazione alla sicurezza online sia incorporata in tutto il programma di studi; garantire che tutto il personale sia a conoscenza delle procedure che devono essere seguite in caso di incidente per la sicurezza online; garantire che sia tenuto un registro di incidenti di sicurezza online; facilitare la formazione e la consulenza per tutto il personale; coordinare con le autorità locali e le agenzie competenti; controllare la condivisione di dati personali; controllare l'accesso a materiali illegali / inadeguati; controllare probabili azioni di cyberbullismo.
L'Animatore Digitale ed il suo team	pubblicare la E-Safety Policy sul sito della scuola; diffusione delle E-Safety Policy attraverso presentazioni al pc e schede semplificative; garantire che tutti i dati relativi agli alunni pubblicati sul sito siano sufficientemente tutelati.

Gli insegnanti	inserire tematiche legate alla sicurezza online in tutti gli aspetti del programma di studi e di altre attività scolastiche; supervisionare e guidare gli alunni con cura quando sono impegnati in attività di apprendimento che coinvolgono la tecnologia online; 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.
Il personale scolastico	comprendere e contribuire a promuovere politiche di e-sicurezza; essere consapevoli dei problemi di sicurezza online 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 al responsabile della sicurezza online; usare comportamenti sicuri, responsabili e professionali nell'uso della tecnologia; garantire che le comunicazioni digitali con gli studenti dovrebbero essere a livello professionale e solo attraverso i sistemi scolastici, non attraverso meccanismo personali, per esempio -mail, telefoni cellulari, ecc.
Gli alunni	leggere, comprendere, era 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 inappropriato; sapere quali azioni intraprendere se loro o qualcuno che conoscono si sente preoccupato o vulnerabile quando si utilizza la tecnologia online; conoscere e capire la politica relativa all'uso dei telefoni cellulari, fotocamere digitali e dispositivi portatili; conoscere e capire la politica della scuola sull'uso di immagini e il cyberbullismo; capire l'importanza di adottare buone pratiche di sicurezza online quando si usano le tecnologie digitali cuori dalla scuola; assumersi la responsabilità di conoscere i benefici e i rischi di utilizzo di Internet e di altre tecnologie in modo sicuro, sia a scuola che a casa.

I genitori	sostenere la scuola nel promuovere la sicurezza online e approvare l'accordo di E-Safety Policy con la scuola; leggere, comprendere e controfirmare il suddetto accordo; accedere al sito web della scuola in conformità con quanto stabilito dalla stessa; assicurarsi che la scuola abbia preso tutte le precauzioni necessarie circa un uso corretto della tecnologia da parte degli alunni.

Al fine di garantire una gestione il più possibile corretta, la scuola attua le seguenti strategie:
Il Dirigente Scolastico si riserva, sentiti i responsabili, di limitare l'accesso e l'uso della rete interna ed esterna secondo i normali canali di protezione presenti nei sistemi operativi.
Si attrezza per evitare comportamenti che non rientrano nelle norme che il Collegio dei Docenti delinea in proposito, come:

- scaricare file video-musicali protetti da copyright;
- visitare siti non necessari ad una normale attività didattica;
- alterare i parametri di protezione dei computer in uso;
- utilizzare la rete per interessi privati e personali che esulano dalla didattica;
- non rispettare le leggi sui diritti d'autore;
- navigare su siti non accettati dalla protezione interna della scuola.

Disposizioni, comportamenti, procedure:

- il sistema informatico è periodicamente controllato dai responsabili (DSGA e docente responsabile su nomina del Dirigente Scolastico).
- la scuola può controllare periodicamente i file utilizzati, i file temporanei e i siti visitati da ogni macchina.
- la scuola archivia i tracciati del traffico internet.
- e' vietato installare e scaricare da internet software non autorizzati.
- le postazioni PC in ambiente Windows sono protette da software che impediscono modifiche ai dati memorizzati sul disco fisso interno.
- al termine di ogni collegamento la connessione deve essere chiusa.
- verifiche antivirus sono condotte periodicamente sui computer e sulle unità di memorizzazione di rete.
- l'utilizzo di CD, chiavi USB e floppy personali deve essere autorizzato dal docente e solo previa scansione antivirus per evitare qualsiasi tipo di infezione alla rete d'Istituto.
- la scuola si riserva di limitare il numero di siti visibili e le operazioni di download.
- Il materiale didattico dei docenti può essere messo in rete, anche su siti personali collegati all'Istituto, sempre nell'ambito del presente regolamento e nel rispetto delle leggi.

Condivisione e comunicazione della Policy all'intera comunità scolastica.
La E-Safety Policy d'Istituto si applica a tutti i membri della scuola, compreso il personale, gli studenti, i genitori, gli utenti della comunità, che ne hanno accesso.

Il Dirigente Scolastico regola il comportamento degli studenti e autorizza i membri del personale di imporre sanzioni disciplinari per il comportamento inadeguato. Questo è pertinente a episodi di cyberbullismo, o altri tipi di incidenti che possono danneggiare la sicurezza online.

La scuola si occuperà di tali incidenti all'interno di questa Policy, delle politiche di comportamento e anti-bullismo associati ed avrà il compito di informare i genitori di episodi di comportamento inappropriato di sicurezza online, che si svolgono all'interno della scuola.

La Policy sarà comunicata al personale, agli alunni, alla comunità nei seguenti modi:

- pubblicazione della E-Safety Policy sul sito dalla scuola;
- accordo di utilizzo accettabile, discusso con gli studenti e i genitori, all'inizio del primo anno, tramite il Patto di Corresponsabilità, che sarà sottoscritto dalle famiglie e rilasciato dalle stesse;
- accordo di utilizzo accettabile rilasciato al personale scolastico.

Gestione delle infrazioni alla Policy.

La scuola prenderà tutte le precauzioni necessarie per garantire la sicurezza online. Tuttavia, a causa della scala internazionale collegata ai contenuti internet, la disponibilità di tecnologie mobili e velocità di cambiamento, non è possibile garantire che il materiale non idoneo apparirà mai su un computer della scuola o dispositivo mobile,. Nè la scuola né l'autorità locale possono accettare la responsabilità per il materiale accessibile, o le conseguenze di accesso a Internet.
Al personale e agli alunni saranno date informazioni sulle infrazioni in uso e le eventuali sanzioni. Le suddette sanzioni includono:

- informare il docente della classe, il docente responsabile della sicurezza online (o il DSGA), il Dirigente Scolastico;
- informare i genitori o i tutori;
- il ritiro del cellulare fino a fine giornata;
- la rimozione di Internet o del computer di accesso per un periodo;
- la comunicazione alle autorità competenti.

Il docente responsabile della sicurezza online fungerà da primo punto di contatto per qualsiasi reclamo. Qualsiasi lamentela personale di abuso sarà riferita al Dirigente Scolastico.
Denunce di bullismo online saranno trattate in conformità con la legge attuale. Reclami relativi alla protezione dei bambini saranno trattati in conformità alle procedure di protezione dell'infanzia.

Monitoraggio dell'implementazione della Policy e suo aggiornamento.
La E-Safety Policy si inserisce all'interno di altre politiche scolastiche, quali la politica di protezione dei minori, la politica anti-bullismo, la politica del benessere degli alunni a scuola.
La scuola ha un docente responsabile della sicurezza online che si prenderà cura della revisione e/o aggiornamento della Policy sotto la supervisione del Dirigente Scolastico.
La E-Safety Policy sarà riesaminata annualmente o quando si verificano cambiamenti significativi per quanto riguarda le tecnologie in uso all'interno della scuola e tutte le modifiche della Policy saranno discusse in dettaglio con tutti i membri del personale docente.

Nell'ambito della revisione della Policy, tutte le informazioni e le revisioni saranno memorizzate per eventuali controlli, sulla base del seguente documento:

Nome	E-Safety Policy I.C. Raffaello Sanzio Falconara Marittima
Versione	1.0
Data	GG/MM/AAAA
Autore	nome del docente responsabile della sicurezza online (E-Safety Policy)
Approvato dal Dirigente	
Approvato dal Collegio docenti	
Prossima data di revisione	

Modifica

Versione	Data	Descrizione	Nome del docente responsabile E-Safety Policy

Nell'ambito del monitoraggio dell'implementazione della E-Safety Policy si terranno in considerazione i dati annuali sulla base del seguente documento:

ANNO	NUMERO DI SEGNALAZIONI	NUMERO DI INFRAZIONI	NUMERO DI SANZIONI DISCIPLINARI
a.s. ...../...			

Integrazione della Policy con Regolamenti esistenti.

2. Formazione e Curricolo

Il Piano Nazionale Scuola Digitale (PNSD) ha l'obiettivo di modificare gli ambienti di apprendimento per rendere l'offerta formativa di ogni Istituto coerente con i cambiamenti della società della conoscenza e con le esigenze e gli stili cognitivi delle nuove generazioni. Il PNSD, con valenza pluriennale, è quindi un'opportunità per innovare la

Scuola, adeguando non solo le strutture e le dotazioni tecnologiche a disposizione dei docenti e dell'organizzazione, ma soprattutto le metodologie didattiche e le strategie usate con gli alunni in classe.
Il DM 851 del 27/10/2015, in attuazione dell'art.1, comma 56 della legge 107/2015, ne ha previsto l'attuazione al fine di:

- migliorare le competenze digitali degli studenti anche attraverso un uso consapevole delle stesse;
- implementare le dotazioni tecnologiche della scuola al fine di migliorare gli strumenti didattici e laboratoriali ivi presenti;
- favorire la formazione dei docenti sull'uso delle nuove tecnologie ai fini dell'innovazione didattica;
- individuare un Animatore Digitale ed un team per l'innovazione digitale che supporti ed accompagni adeguatamente l'innovazione didattica, nonché l'attività dell'animatore digitale;
- partecipare a bandi nazionali ed europei per finanziare se suddette iniziative;

Curricolo sulle competenze digitali per gli studenti.
Nell'ambito del PNSD questa scuola si propone un programma di progressiva educazione alla sicurezza online, come parte del curriculum scolastico. Si impegna a sviluppare una serie di competenze e comportamenti adeguati alle età degli alunni e ad esperienze, tra cui:

- programmare attività e far partecipare gli alunni a laboratori di Coding in occasione della settimana del codice;
- sviluppare una serie di strategie per valutare e verificare le informazioni prima di accettare l'esattezza;
- essere a conoscenza che l'autore di un sito/pagina web può avere un particolare pregiudizio;
- sapere come restringere o affinare una ricerca;
- capire il comportamento accettabile quando si utilizza un ambiente online, vale a dire, essere educato, non utilizzare comportamenti inappropriati, mantenere le informazioni personali private;
- capire come le fotografie possono essere manipolate e individuare contenuti web in grado di attrarre il tipo sbagliato di attenzione;
- capire perché "amici" online potrebbero non essere chi dicono di essere e di comprendere perché dovrebbero fare attenzione in un ambiente online;
- capire il motivo per cui non dovrebbero inviare o condividere resoconti dettagliati delle loro vite personali e informazioni di contatto;
- capire il motivo per cui non devono pubblicare foto o video di altri senza il loro permesso;
- sapere di non scaricare alcun file, come i file musicali, senza permesso;
- comprendere l'impatto di bullismo online, sexting, gromming e sapere come cercare aiuto se sono in pericolo;
- sapere come segnalare eventuali abusi tra cui il bullismo online e come chiedere aiuto ai docenti, ai genitori, se si verificano problemi quando si utilizzano le tecnologia internet;
- utilizzare con attenzione internet per garantire che si adatti alla loro età e supporti gli obiettivi di apprendimento per le aree curriculari specifiche.

Formazione dei docenti sull'utilizzo e l'integrazione delle TIC nella didattica.

Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali

Nell'ambito del PNSD questa scuola ha previsto:

- individuazione e formazione di un Animatore Digitale che come docente accompagnerà il Dirigente Scolastico e il Direttore S.G.A. nell'attuazione degli obiettivi e delle innovazioni previste dal PSND;
- formazione dei docenti all'utilizzo del registro elettronico e dello scrutinio elettronico;
- somministrazione di un questionario rivolto ai docenti per la rilevazione dei bisogni digitali;
- realizzazione/ampliamento della rete WI-Fi/LAN nei plessi dell'Istituto;
- ricognizione e messa a punto delle dotazioni digitali;
- attivazione e comunicazione di iniziative di formazione, in particolare rivolte allo sviluppo e alla diffusione del Coding e del pensiero computazionale;
- monitoraggio del piano digitale di Istituto e dei risultati conseguiti;
- si assicura che il personale sa come inviare o ricevere dati sensibili o personali e comprendere l'obbligo di crittografare i dati dove la sensibilità richiede protezione degli stessi;
- offre una formazione a disposizione del personale in materia di sicurezza online attraverso corsi di formazione e/o aggiornamento;
- fornisce, come parte del processo di induzione, tutto il nuovo personale con informazioni e indicazioni sulla E-Safety Policy di Istituto.

Sensibilizzazione delle famiglie.

Questa scuola esegue un programma continuativo di consulenza, orientamento e formazione per i genitori tra cui:

- presentare ai genitori, i cui figli si scrivono nel nostro Istituto, il Regolamento della Policy, al fine di garantire che i principi di comportamento sicuro online siano chiari;
- distribuire volantini di informazione e pubblicazioni sul sito della scuola;
- offrire incontri di consulenza con esperti;
- fornire informazioni sui siti nazionali di sostegno per i genitori, quali il sito: www.generazioniconnesse.it

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

- Accesso ad internet: filtri antivirus e sulla navigazione.
  L'Istituto dispone di una rete interna protetta da Firewall per quanto riguarda le connessioni con l'esterno. Le postazioni sono protette con sistemi antivirus regolarmente aggiornati .
- L'Istituto dispone di una rete con tecnologia senza fili. L'accesso alla rete wireless è regolato tramite password. Gli studenti possono accedere alla rete con account Studenti.
-
- Gestione accessi (password, backup, ecc.).
- L'accesso alla rete wireless è regolato tramite password.
-
- E-mail.
  questa scuola non pubblica indirizzi di posta elettronica personali degli alunni o del personale sul sito della scuola. Sarà contattato il Dirigente Scolastico se qualcuno dello staff o degli alunni riceve una e-mail che consideriamo

particolarmente preoccupante o che infrange la legge.
Farà rapporto di attività illegali alle competenti autorità e, se necessario, alla polizia.

- Sa che spam, phishing e virus allegati possono rendere le mail pericolose. Perciò si utilizzeranno una serie di tecnologie per proteggere utenti e sistemi nella scuola, tra cui anti-virus, oltre al filtraggio delle email.
-
- Blog e sito web della scuola
- L'istituto dispone di un proprio spazio web e di un proprio dominio.
- L'istituto gestisce un proprio sito web nello spazio di proprietà. La gestione del sito della scuola e la rispondenza alle normative per quanto concerne i contenuti (accuratezza, appropriatezza, aggiornamento) e le tecniche di realizzazione e progettazione è a cura del Webmaster. La scuola detiene i diritti d'autore dei documenti che si trovano sul proprio sito o di quei documenti per i quali è stato chiesto ed ottenuto il permesso dall'autore proprietario. Le informazioni pubblicate sul sito della scuola relative alle persone da contattare rispetteranno le norme vigenti sulla privacy.
- 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.
-
- Social network.
- L'istituto dispone di un canale Youtube, nel quale vengono caricati video didattici e video informativi delle attività svolte durante l'anno.
-
- Protezione dei dati personali.

4. Strumentazione personale
   - Per gli studenti: gestione degli strumenti personali - cellulari, tablet ecc..
     Come da Regolamento d'Istituto agli studenti è vietato l'utilizzo del cellulare all'interno della scuola. Per quanto concerne l'utilizzo dei tablet, questi possono essere utilizzati solo alla presenza del docente e per ragioni prettamente scolastiche.
   -
   - Per i docenti: gestione degli strumenti personali - cellulari, tablet, notebook ecc..
     I docenti possono utilizzare cellulari, tablet e notebook a scopo personale non durante l'attività didattica o lavorativa.

   - Per il personale della scuola: gestione degli strumenti personali - cellulari, tablet, notebook ecc..
     Il personale della scuola può utilizzare cellulari, tablet e notebook a scopo personale non durante l'attività didattica o lavorativa.
   -

5. Prevenzione, rilevazione e gestione dei casi

Prevenzione

Principi generali

- internet favorisce la libertà di 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;
    - 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.
    - 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 alla risposta non banale.
    - 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.
    - 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.
    - 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 educhi 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.

Rischi
Forme online di bullismo
La forma online di bullismo (cyberbullismo) ha alcune caratteristiche peculiari che lo rendono pericoloso perché:
- il cyberbullismo è pervasivo: può raggiungere la sua vittima in qualsiasi momento e in qualsiasi luogo. La possibilità di avere smartphone sempre accesi e spesso connessi ad internet permette al cyberbullo di aggredire la sua vittima ogni volta che lo desidera;
- è un fenomeno persistente: il materiale diffamatorio pubblicato su internet può rimanere disponibile online anche per molto tempo;
- spettatori e cyberbullli sono potenzialmente infiniti: le persone che possono assistere ad episodi di cyberbullismo sono potenzialmente illimitate e molti possono essere cyberbulli, anche solo condividendo o promuovendo l'episodio di cyberbullismo, che finisce per replicarsi (ad esempio sulle bacheche dei profili che i ragazzi hanno sui social network) in modo incontrollabile.

Azioni
La scuola si impegna a:
- riconoscere il Dirigente Scolastico come titolare del trattamento di dati personali secondo la Legge sulla privacy (art.41 del D.Lgs. 196/2003);
- riconoscere come responsabili della sicurezza online il DSGA ed un docente su nomina del Dirigente Scolastico;
- nominare l'Animatore Digitale ed il team che lo affiancherà, su nomina del Dirigente Scolastico dopo richiesta di disponibilità fatta con circolare.
- creare uno sportello di ascolto interno all'Istituto aperto ad alunni, genitori, docenti.
- Seguire, diffondere e fare proprie le "Linee di orientamento per azioni di prevenzione e contrasto al bullismo e al cyberbullismo" emanate dal Miur nell'Aprile 2015 e il "Manifesto della Comunicazione non Ostile": una carta che raccoglie 10 princìpi di stile scritto a più mani dalla community "Parole O_Stili"con l'obiettivo di ridurre, arginare e combattere i linguaggi negativi che si propagano facilmente in Rete. Il manifesto si rivolge a tutti gli utenti di internet: giovani e adulti, esperti e non.
I contenuti del manifesto sono:

Virtuale è reale : dico o scrivo in reto solo cose che ho il coraggio di dire di persona.
Si è ciò che si comunica: le parole che scelgo raccontano la persona che sono: mi rappresentano.
Le parole danno forma al pensiero: mi prendo tutto il tempo necessario a esprimere al meglio quello che penso.
Prima di parlare bisogna ascoltare: nessuno ha sempre ragione, neanche io. Ascolto con onestà e apertura.
Le parole sono un ponte: scegli le parole per comprendere, farmi capire, avvicinarmi agli altri.
Le parole hanno conseguenze: so che ogni mia parola può avere conseguenze, piccole o grandi.
Condividere è una responsabilità: condivido testi e immagini solo dopo averli letti, valutati, compresi.
Le idee si possono discutere. Le persone si devono rispettare: non trasformo chi sostiene opinioni che non condivido in un nemico da annientare.
Gli insulti non sono argomenti: non accetto insulti e aggressività, nemmeno a favore della mia tesi.

Anche il silenzio comunica: quando la scelta migliore è tacere, taccio.

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 cyberbullismo;
- creare degli spazi in cui gli alunni si possano confrontare su questo tema, utilizzando come spunti di riflessione: film, canzoni, materiali prodotti da altri alunni;
- mantenere viva una task-force interna all'istituto, che possa progettare attività formative sul fenomeno del cyberbullismo e calenydarizzarle per tutta la comunità scolastica;
- confrontarsi con gli altri insegnanti della classe, della scuola o con esperti del territorio;
- rivolgersi alla helpline di generazioni connesse.
- Seguire, diffondere e fare proprie le "Linee di orientamento per azioni di prevenzione e contrasto al bullismo e al cyberbullismo" emanate dal Miur nell'Aprile 2015 e il "Manifesto della Comunicazione non Ostile": una carta che raccoglie 10 princìpi di stile scritto a più mani dalla community "Parole O_Stili"con l'obiettivo di ridurre, arginare e combattere i linguaggi negativi che si propagano facilmente in Rete. Il manifesto si rivolge a tutti gli utenti di internet: giovani e adulti, esperti e non.

I genitori si impegnano a:
- firmare il patto di Corresponsabilità redatto dalla scuola;
- prendere visione della E-Safety Policy messa a disposizione di docenti, genitori ed alunni sul sito della scuola;
- 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 del Patto di Corresponsabilità che i genitori hanno firmato con la scuola;
- 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
Intervenire in situazioni di cyberbullismo non è mai semplice: spesso si pensa di non sapere esattamente cosa fare e si ha il timore di essere inadeguati. Per tale motivo la scuola si impegna ad individuare due strumenti che potranno agevolare l'intera comunità scolastica:
- nel decidere come intervenire;
- nel tenere traccia di ciò che è avvenuto rispetto ai comportamenti degli alunni online e di come è stato gestito il problema.

L'obiettivo a lungo termine, che come comunità scolastica ci diamo, è quello di creare una memoria condivisa non solo di ciò che accade nella scuola rispetto al web, ma anche di strutturare una fonte esemplificativa che possa orientare sempre più e sempre meglio le azioni di contrasto ad episodi che, nel tempo, potrebbero ripetersi.

Gestione dei casi
Per una efficace gestione dei casi la scuola si riserva di utilizzare lo schema messo a disposizione dal sito www.generazioniconnesse.it (Allegato n.1).

Per poter tenere traccia di ciò che è avvenuto rispetto ai comportamenti degli alunni online e di come è stato gestito il problema, la scuola si riserva di utilizzare il "Diario di Bordo" messo a disposizione dal sito www.generazioniconnesse.it (Allegato n.2).

La Scuola si impegna inoltre ad organizzare le seguenti attività di prevenzione al fenomeno:
- organizzazione di Corsi di formazione per docenti, genitori, operatori del settore socio-educativo;
- monitoraggio sul tema del cyberbullismo attraverso questionari (Allegato n.3);
- partecipazione da parte di docenti, studenti e genitori a convegni e seminari sul tema del bullismo e del cyberbullismo;
- interventi di consulenza e supporto (su richiesta da parte della scuola) relativamente a casi di cyberbullismo.

Annessi (da prodursi a cura della scuola)
- Procedure operative per la gestione delle infrazioni alla Policy (Allegato n.4).
- Procedure operative per la rilevazione, il monitoraggio e la gestione delle segnalazioni (Allegato n. 1; Allegato n. 2; Allegato n. 3).

Firma Referente

Monica Ciminaghi

Il Dirigente Scolastico

IL DIRIGENTE SCOLASTICO
Francesco Maria Orsolini

Sicurezza in rete - Schema per la scuola

Cosa fare in caso di... cyberbullismo?

Alunno/a preso in giro/minacciato/offeso online

- Se gli alunni coinvolti sono d'accordo, **informa** i genitori
- **Coinvolgi** il referente di istituto dell'e-safety e gli operatori scolastici su quanto sta accadendo
- **Segnala** alla **polizia postale** [segnala: a) contenuto b) modalità di diffusione].
- **Coinvolgi** la comunità scolastica in percorsi di prevenzione dei comportamenti a rischio online
- **Tieni traccia** di quanto successo e delle azioni intraprese: **compila il diario di bordo**

- **Dialoga** (con la classe - 1): Parla del cyberbullismo e delle sue conseguenze (non nominare gli alunni coinvolti). Insegna loro a **chiedere aiuto** per situazioni di questo tipo.
- **Dialoga** (con la classe - 2): Chiedi agli alunni coinvolti di intervenire per far terminare le prese in giro: il loro silenzio asseconda quanto sta accadendo.
- Parla della necessità di **non diffondere** ulteriormente online i materiali.
- Informa gli alunni su ciò che dice la **legge italiana** sul cyberbullismo, che è reato.
- **Previeni** (con la classe - 3): Proponi attività in classe sull'empatia e sul riconoscimento delle emozioni (proprie e altrui)
- Quando il cyberbullismo termina, coinvolgi il team e-safety sulle **azioni** appropriate per prevenire altre situazioni di rischio

- **La situazione richiede delicatezza**: cerca di capire meglio cosa sta succedendo.
  - Se è opportuno, richiedi un sostegno ai servizi territoriali o ad altre Autorità competenti (soprattutto se il cyberbullismo non si limita alla scuola)

- **Chiedi un consiglio** telefonico alla **helpline** del progetto Generazioni Connesse al numero gratuito **1.96.96**






Co-financed by the European Union
Connecting Europe Facility

Generazioni Connesse

Schema riepilogativo delle situazioni gestite legate a rischi online

Riepilogo casi
Scuola_____ Anno Scolastico_____

N°	Data	ora	Episodio *(riassunto)*	Azioni intraprese		Insegnante con cui l'alunno/a si è confidato	Firma
				Cosa?	Da chi?		

ALLEGATO N. 3

QUESTIONARIO

Ti preghiamo di rispondere con sincerità a tutte le domande e di lavorare autonomamente senza commentarle con i compagni. Le tue risposte saranno molto importanti per migliorare la vita dei ragazzi a scuola.
Ti ricordiamo che i questionari non sono un compito scolastico, non esiste una risposta giusta o sbagliata, quella più immediata e spontanea è la migliore!
Le risposte ai questionari sono confidenziali e non sarà mai possibile risalire al tuo nome e che sei libero di rifiutarti di rispondere.
Se vorrai, dopo potremmo discutere del questionario insieme ai tuoi insegnanti.
Nessuno a scuola o a casa saprà in che modo hai risposto a queste domande.
Molte domande riguardano la tua vita a scuola dal momento in cui è iniziata, cioè a partire da settembre.
Quando rispondi cerca di pensare a tutto questo e non soltanto agli ultimi giorni o mesi.

Ora puoi procedere.

Ti ringraziamo per la collaborazione

SESSO Maschile Femminile

Cyberbullismo
Il cyberbullismo è una nuova forma di prepotenza che prevede l'utilizzo di email, messaggi di testo, chat, siti web, telefoni cellulari o altre forme di informazione tecnologica allo scopo di tormentare, minacciare o intimidire qualcuno, diffondere dicerie e storie non vere sul conto di altri.
Il cyberbullismo può includere alcune azioni come minacce, insulti su diversa razza e ripetuta vittimizzazione di qualcuno tramite supporto elettronico.

1. Conosci qualcuno che ha subito prepotenze attraverso il cyberbullismo in questo anno scolastico?

   - No
   - Si, a scuola
   - Si, fuori dalla scuola
   - Si, sia da compagni della scuola che da quelli fuori la scuola

2. Hai mai subito prepotenze attraverso il cyberbullismo in questo anno scolastico?

   - No
   - Si, dai compagni di scuola
   - Si, dai compagni fuori dalla scuola
   - Si, sia da compagni della scuole che da quelli fuori la scuola

3. Che tipo di esperienza hai avuto?

	Mai	Solo 1 volta o 2	2-3 volte al mese	1 volta a settimana	Diverse volte alla settimana
Mi sono arrivati brutti messaggi (facendo minacce e commenti)					
Foto/video offensivi sul cellulare					
Mi hanno fatto scherzi o telefonate mute					
Attraverso cattive o brutte email					
Hanno diffuso riprese o foto di mie situazioni imbarazzanti o intime su internet o con il telefonino					
Hanno diffuso dicerie sul mio conto tramite web e/o Sms, chat, facebook ...					
Ho ricevuto insulti sulla rete					
Altro (scrivi cosa)					

4. Hai mai preso parte ad episodi di cyberbullismo in questo anno scolastico?

- No
- Qualche volta
- Spesso

5. A che tipo di comportamento hai preso parte in questo anno scolastico)

	Mai	Solo 1 volta o 2	2-3 volte al mese	1 volta a settimana	Diverse volte alla settimana
Inviare (ho inviato) brutti messaggi di testo (facendo minacce e commenti)					
Foto/video offensivi sul cellulare					
Scherzi o telefonate mute					
Inviare (ho inviato) cattive o brutte e-mail					
Diffondere riprese o foto di situazioni imbarazzanti o intime su internet o con il telefonino					
Diffondere dicerie sul conto di altri tramite web e/o Sms, chat, Facebook..... Insultare sulla rete					
Altro (scrivi cosa)					

Allegato N. 4

Procedure operative per la gestione delle infrazioni alla E-Safety Policy

Ogni volta che un membro del personale o studente viola la E-Safety Policy, la decisione finale sul livello di sanzioni sarà a discrezione del Dirigente scolastico e rifletterà le procedure comportamentali e disciplinari della scuola.
Di seguito sono fornite solo come esemplificazione:

STUDENTI

INFRAZIONI	POSSIBILI SANZIONI
- L'uso di siti non educativi durante le lezioni; - l'utilizzo non autorizzato di e-mail; - l'uso non autorizzato del telefono cellulare (o altre nuove tecnologie) durante le lezioni. - Uso di instant messaging /siti di social networking.	Fare riferimento all'insegnante della classe/ docente responsabile della sicurezza online/Dirigente Scolastico
- L'uso continuato di siti non educativi durante le lezioni dopo essere stato avvertito; - l'uso non autorizzato di email dopo essere stato avvertito. - l'uso non autorizzato del telefono cellulare (o altre nuove tecnologie) dopo essere stato avvertito. - l'uso continuato di messaggistica/chat istantanea, siti di social networking, newsgroup. - l'uso di materiale offensivo.	Fare riferimento all'insegnante della classe/docente responsabile della sicurezza online/Dirigente scolastico. Escalation: - rimozione dei diritti di accesso a internet per un periodo; - rimozione di telefono fino a fine giornata; - contatto con i genitori.
- Rovinare o distruggere deliberatamente i dati di qualcuno, violare la privacy altrui o messaggi inappropriati, video o immagini su un sito di social networking. - invio di un messaggio email o MSN o chat che è considerato molestia o azione di bullismo. - Cercare di accedere a materiale offensivo o pornografico.	Fare riferimento all'insegnante della classe/docente responsabile della sicurezza online/Dirigente Scolastico Escaltation: - rimozione dei diritti di accesso a Internet per un periodo; - rimozione del telefono fino a fine giornata; - contatto con i genitori; - contattare le autorità competenti.
- Invio di email o messaggi di Msn o chat considerati molestia o bullismo dopo essere stato avvertito; - accedere deliberatamente allo scaricamento o alla diffusione di qualsiasi materiale ritenuto offensivo, osceno, diffamatorio, razzista, omofonico o violento. - trasmissione di materiale che viola i diritti d'autore di un'altra persona o infranga le condizioni della legge sulla protezione dei dati. - portare il nome della scuola in discredito	Fare riferimento all'insegnante della classe/ contatto con i genitori Altre possibili azioni di salvaguardia: - conservare le prove; - informare i provider di servizi di posta elettronica del mittente; - fare rapporto alle autorità competenti dove si sospetti la pedofilia o altre attività illegali.

PERSONALE SCOLASTICO

INFRAZIONI	POSSIBILI SANZIONI
- L'uso di internet per attività personali non legate allo sviluppo professionale (shopping online, email personali, instante messalina, chat, ecc) - l'utilizzo di supporti di memorizzazione dei dati personali (ad esempio chiavetta Usb) senza considerare l'accesso e l'adeguatezza di qualsiasi file memorizzato; - non implementare adeguate procedure di salvaguardia; - qualsiasi comportamento su web che compromette la professionalità del personale nella scuola e nella comunità. - l'uso improprio di primo livello di sicurezza dei dati, ad esempio uso illecito di password; - violazione del copyright o della licenza per l'installazione di software.	Fare riferimento al docente responsabile della sicurezza online/DSGA//Dirigente Scolastico. Escalation a: -avvertimento
- Gravi danni intenzionali all'hardware o software del computer; - qualsiasi tentativo deliberato di violare la protezione dei dati o di sicurezza informatica; - creare, accedere, scaricare e diffondere deliberatamente qualsiasi materiale ritenuto offensivo, osceno, diffamatorio, razzista, omofonico o violento; - ricevere o trasmettere materiale che viola i diritti d'autore di un'altra persona o infranga le condizioni della legge sulla protezione dei dati; - portare il nome della scuola in discredito.	Fare riferimento al docente responsabile della sicurezza online/DSGA/Dirigente scolastico. Altre azioni di salvaguardia: - trasferire il pc in un luogo sicuro per garantire che non vi è alcun ulteriore accesso al Pc o laptop; - far verificare tutte le attrezzature per garantire che non vi è alcun rischio di alunni che accedono a materiali inappropriati nella scuola. - Escalation: - contattare e fare rapporto alle autorità competenti. -

Come saranno informati il personale e gli studenti di queste procedure?

- la E-Safety Policy sarà resa disponibile sul sito dell'Istituto a studenti, personale scolastico e genitori.
- i genitori firmeranno la E-Safety Policy quando il loro bambino inizierà la scuola.
- agli studenti sarà insegnato un uso responsabile della rete in modo tale che possano sviluppare "comportamenti sicuri".
- informazioni su come segnalare azioni di bullismo o cyberbullismo saranno messe a disposizione della scuola per gli alunni, il personale e i genitori.