MINISTERO DELL'ISTRUZIONE, DELL'UNIVERSITÀ E DELLA RICERCA
Ufficio Scolastico Regionale per il Lazio
ISTITUTO COMPRENSIVO "PIAZZA BORGONCINI DUCA 5"
Piazza F. Borgoncini Duca, 5 - 00165 ROMA (RM)
Tel. 066390421 – Fax/Tel. 066374351
e mail: rmic847005@istruzione.it – rmic847005@pec.istruzione.it
Distretto Scolastico 26° - cod. fisc. 97198560589
sito: www.icborgonciniducaroma.com

E- Safety Policy

INTRODUZIONE

La Dichiarazione dei diritti in internet del 2015 garantisce, quale diritto fondamentale delle persone, il pieno riconoscimento di libertà, eguaglianza, dignità e diversità di ciascuno. Internet è oggi lo strumento essenziale per promuovere la partecipazione individuale e collettiva ai processi democratici e l'eguaglianza sostanziale. Le istituzioni sono chiamate in causa per promuovere l'educazione all'uso consapevole del web e per rimuovere ogni forma di ritardo culturale che precluda o limiti l'utilizzo di Internet da parte delle persone (Art. 3, comma 4). Tuttavia, se non adeguatamente gestito, Internet può divenireuno strumento che limita i diritti personali e favorisce i comportamenti a rischio e lesivi della libertà altrui (Art. 3, comma 5).

I numerosi episodi di bullismo e cyberbullismo che coinvolgono gli studenti del territorio nazionale impongono la necessità di una presa in carico significativa da parte della scuola. Il Ministero dell'Istruzione, dell'Università e della Ricerca, come misura di intervento, ha emanato la legge 71 del 29 maggio 2017 che "si pone l'obiettivo di contrastare il fenomeno del cyberbullismo in tutte le sue manifestazioni, con azioni a carattere preventivo e con una strategia di attenzione, tutela ed educazione nei confronti dei minori coinvolti, sia nella posizione di vittime sia in quella di responsabili di illeciti, assicurando l'attuazione degli interventi senza distinzione di eta' nell'ambito delle istituzioni scolastiche" (Art.1 comma 1). Le successive linee di orientamento, pubblicate il 26 ottobre 2017, e che hanno lo scopo di attuare le finalità dell'art.1, comma , includono per il triennio 2017-2019: la formazione del personale scolastico, prevedendo la partecipazione di un proprio referente per ogni autonomia scolastica; la promozione di un ruolo attivo degli studenti, nonche' di ex studenti che abbiano gia' operato all'interno dell'istituto scolastico in attivita' di peer education, nella prevenzione e nel contrasto del cyberbullismo nelle scuole; la previsione di misure di sostegno e rieducazione dei minori coinvolti. Le suddette linee:

- definiscono gli interventi per la prevenzione e il contrasto del fenomeno;
- evidenziano l'iniziativa del progetto Generazioni connesse e altri strumenti utili per un uso corretto e consapevole delle tecnologie digitali;
- suggeriscono le modalità di segnalazione di situazioni e/o comportamenti a rischio;
- definiscono le misure di Governance;
- indirizzano le scuole sulle azioni rivolte agli studenti e alle loro famiglie e
- delineano il ruolo del Dirigente scolastico e del docente referente.

Scopo della E-Policy

L'Istituto Comprensivo Borgoncini Duca ha da tempo incrementato l'uso delle tecnologie

informatiche nella didattica, attraverso la dotazione di LIM in tutte le aule dei tre plessi, e nell'organizzazione generale della scuola. Internet è diventato lo strumento privilegiato sia per svolgere esperienze formative, sia per condurre in modo più efficiente le funzioni amministrative, grazie all'implementazione costante del sito internet della scuola, all'introduzione del registro elettronico e all'utilizzo della piattaforma web Scuola365 che consente di gestire in modo più immediato il sistema-scuola ed offre all'utenza una comunicazione più tempestiva, chiara e trasparente. Gli insegnanti, gli alunni e tutto il personale che vive il mondo della scuola costituiscono una comunità e, come tale, sono tenuti a seguire i principi fondamentali che regolano l'utilizzo delle tecnologie. Sono tenuti anche a conoscere

La scuola ha aderito al progetto "Generazioni Connesse" (www.generazioniconnesse.it) e si è attivata nell'elaborazione di linee guida per una e-Safety Policy d'Istituto, cioè di un proprio codice di condotta nella prevenzione e gestione dei casi di (cyber)bullismo e di un regolamento di sicurezza informatica, che diventerà parte integrante del Regolamento di Istituto.

Questa E-Policy si pone i seguenti obiettivi:

- salvaguardare e proteggere i bambini, i ragazzi e il personale dell'istituto;
- assistere il personale della scuola nell'utilizzo delle TIC e nel monitoraggio del proprio lavoro attraverso esse;
- impostare precisi codici di condotta rilevanti per l'uso responsabile di internet, sia a scopo didattico che personale e ricreativo;
- affrontare situazioni di abuso online e cyberbullismo;
- garantire che tutti i membri della comunità scolastica abbiano consapevolezza del fatto che i comportamenti illeciti e/o pericolosi sono considerati inaccettabili e che saranno oggetto di sanzioni disciplinari e giudiziarie.

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

Tutti i membri della comunità scolastica sono chiamati in causa, a seconda del proprio ruolo e della propria responsabilità:

Dirigente scolastico

L'art. 5 della L. 71/2017 prevede che "nell'ambito della promozione degli interventi finalizzati ad assicurare la qualità dei processi formativi e la collaborazione delle risorse culturali, professionali, sociali del territorio, il dirigente scolastico, definisca le linee di indirizzo del Piano Triennale dell'Offerta Formativa (PTOF) e del Patto di Corresponsabilità (D.P.R. 235/07) affinché contemplino misure specificatamente dedicate alla prevenzione del cyberbullismo" (Linee di orientamento sul cyberbullismo, Miur, ottobre 2017). Il DS ha, quindi, responsabilità in merito alla

gestione dei dati e alla loro sicurezza; deve garantire che la scuola utilizzi un servizio internet filtrato, approvato e conforme alle leggi vigenti; deve assicurare al personale una formazione adeguata per svolgere i ruoli di sicurezza online e per la formazione di altri colleghi; deve essere a conoscenza delle procedure da attuare nei casi di infrazione della E-Policy; è chiamato a rivedere l'E-Policy e ricevere le relazioni di monitoraggio da parte del responsabile; deve garantire la presenza di un sistema di monitoraggio del personale di supporto che svolge le procedure di sicurezza online interne.

Responsabili della sicurezza online (DSGA e docente referente)

Il DSGA e il docente referente nominato dal DS sono responsabili per i problemi di sicurezza online; promuovono la consapevolezza e l'impegno per la salvaguardia online di tutta la comunità scolastica; assicurano che l'educazione alla sicurezza online sia parte del programma di studi; garantiscono che il personale sia a conoscenza delle procedure da seguire in caso di incidente per la sicurezza online; garantiscono la tracciabilità degli eventuali incidenti su un apposito registro; facilitano la formazione e la consulenza per tutto il personale; coordinano con le autorità locali e le agenzie competenti; controllano la condivisione dei dati personali, l'accesso a materiali inadeguati o illegali e le probabili azioni di cyberbullismo.

Animatore digitale e suo team

All'animatore digitale e al suo team spetta il compito di: pubblicare la E-Safety Policy sul sito della scuola (anche attraverso power point e schede semplificative); garantire che tutti i dati relativi agli alunni pubblicati sul sito siano adeguatamente tutelati.

Insegnanti

Gli insegnanti devono far sì che le tematiche legate alla sicurezza online siano parte del programma di studi e delle altre attività scolastiche; devono supervisionare e guidare gli alunni mentre sono impegnati in attività che utilizzano la tecnologia online; devono garantire che gli studenti siano pienamente consapevoli dei problemi legali relativi ai contenuti del web (es. leggi sul copyright); devono segnalare tempestivamente qualsiasi abuso sospetto o problema al DS e ai responsabili della sicurezza on line (*all. 3 Cosa fare in caso di cyberbullismo; all. 1 modulo di segnalazione;*).

Personale scolastico

Tutto il personale scolastico è chiamato a conoscere e contribuire a promuovere politiche di sicurezza online; deve essere consapevole dei problemi di sicurezza legati all'uso di dispositivi elettronici portatili (cellulari, tablet, fotocamere...), monitorarne l'uso attuando le politiche

scolastiche stabilite; deve segnalare qualsiasi abuso sospetto o problema ai responsabili della sicurezza online; usare comportamenti sicuri, responsabili e professionali nell'uso delle tecnologie; garantire che le comunicazioni con gli studenti avvengano per mezzo dei sistemi scolastici e non utilizzando meccanismi personali.

Alunni

Gli alunni devono comprendere e rispettare la E-Safety Policy; devono acquisire capacità di ricerca nel web, evitando il plagio e rispettando le normative sul diritto d'autore; capire l'importanza di segnalare abusi e l'accesso o l'uso improprio di materiali inappropriati; sapere quali azioni intraprendere se si sentono vulnerabili nell'utilizzo della tecnologia online; conoscere e comprendere la politica relativa all'uso dei telefoni cellulari, fotocamere digitali e dispositivi portatili; conoscere e capire la politica scolastica sull'uso di immagini e cyberbullismo; saper adottare buone pratiche di sicurezza online quando utilizzano le tecnologie digitali fuori dalla scuola; conoscere i benefici e assumersi la responsabilità dei rischi derivanti dall'uso scorretto di internet e delle altre tecnologie, sia a casa che a scuola.

Genitori

Ai genitori spetta il compito di sostenere la scuola e promuovere la sicurezza online, approvando, controfirmandolo, l'accordo di E-Safety Policy con la scuola; devono accedere al sito web della scuola in conformità con quanto stabilito dalla stessa; devono assicurarsi che la scuola abbia preso le precauzioni necessarie per l'utilizzo corretto della tecnologia da parte degli alunni; devono partecipare alle iniziative formative ed informative promosse dalla scuola su tematiche specifiche.

Condivisione e comunicazione della Policy all'intera comunità scolastica

La E-Safety Policy di istituto verrà comunicata al personale, agli alunni, ai genitori e ai diversi utenti della comunità scolastica attraverso:

- pubblicazione sul sito della scuola;
- tramite il Patto di Corresponsabilità, sottoscritto dalla famiglie e rilasciato alle stesse all'inizio dell'anno scolastico.

Gestione delle infrazioni alla Policy

Data l'enorme numerosità dei contenuti in rete, la disponibilità di tecnologie mobili e la velocità di cambiamento, risulta oltremodo impossibile garantire che materiale inappropriato verrà mai visionato su un computer della scuola, ma l'istituto si impegna a prendere tutte le precauzioni necessarie per garantire la sicurezza online dei suoi utenti. Qualsiasi reclamo o denuncia deve

essere trasmessa al docente responsabile della sicurezza online che riferirà al DS. Denunce di cyberbullismo saranno trattate in conformità con la legge attuale; eventuali denunce di violazione della protezione dei bambini saranno trattate in conformità alle procedure di protezione dell'infanzia.

Il personale scolastico e gli alunni saranno informati circa le sanzioni che seguiranno ad eventuali infrazioni, quali:

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

Monitoraggio dell'implementazione della Policy e suo aggiornamento

Il docente responsabile della sicurezza online avrà cura di revisionare e aggiornare l'E-Safety Policy sotto la supervisione del DS. Questa verrà riesaminata ogni anno o in occasione di cambiamenti significativi in merito alle tecnologie in uso all'interno della scuola. Tutte le modifiche saranno condivise con il personale scolastico. Verrà predisposto un documento atto a registrare tutte le revisioni per eventuali controlli.

Allo stesso modo, ai fini del monitoraggio degli episodi, si predisporrà un documento che contenga il numero di segnalazioni, di infrazioni e di sanzioni disciplinari registrare nel corso dell'anno scolastico (all. 2: *diario di bordo*).

2. FORMAZIONE E CURRICOLO

Curricolo sulle competenze digitali degli studenti

In conseguenza della maggiore attenzione rivolta al ruolo delle nuove tecnologie nell’attuale società della conoscenza e dell’informazione, il curricolo prevede modelli di insegnamento e di apprendimento che conducono a percorsi di innovazione didattica attraverso l’introduzione delle TIC come strumenti utili sul piano sia cognitivo (si pensi ad esempio all’uso del pc per scrivere, rielaborare e far interagire il sistema dei saperi), sia sociale (si pensi all’uso di chat, forum, blog, ecc.).

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

Attraverso la definizione dei traguardi delle competenze di base e degli obiettivi di apprendimento

(abilità e contenuti), si punta alla promozione di una didattica per competenze, attenta soprattutto alle competenze digitali per gli studenti, annoverate tra i saperi necessari per la cittadinanza e considerate come un nuovo modello di alfabetizzazione richiesto dalle nuove tecnologie e dalla Rete.

Di conseguenza, anche la formazione dei docenti avrà come obiettivo principale la revisione del modo di fare didattica, individuando nelle TIC solo uno dei possibili strumenti per attuarlo.

Sensibilizzazione delle famiglie

L'integrazione delle TIC e di Internet nella didattica richiede parallelamente una formazione sull'utilizzo consapevole e sicuro degli stessi, da condividere con le famiglie.

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

Le apparecchiature presenti nella Scuola sono un patrimonio comune, quindi, vanno utilizzate con il massimo rispetto, minimizzando gli sprechi di risorse a disposizione. L'utilizzo delle apparecchiature è regolamentato da criteri che puntano a massimizzare la collaborazione collegiale: gli insegnanti sono responsabili delle dotazioni tecnologiche e hanno il compito di responsabilizzare gli alunni per divenire consapevoli dell'importanza della salvaguardia di un bene comune, seguendo le corrette norme di utilizzo.

Gli utenti della scuola utilizzano le dotazioni digitali nei seguenti spazi fisici:

- aule dotate di postazione PC e LIM
- laboratori multimediali a cui accedono sia insegnanti che alunni;
- aule docenti con postazioni complete di lavoro.

Strategie previste dalla scuola per garantire la sicurezza in rete:

- avvio di percorsi di formazione ad un uso consapevole delle dotazioni tecnologiche rivolti agli insegnanti nel corso dell'anno scolastico, in presenza di risorse economiche e umane;
- coinvolgimento dei genitori come partner educativi nei percorsi di formazione che riguardano gli studenti;
- diffusione di una costante e aggiornata informazione agli utenti sui pericoli della rete in relazione all'evoluzione delle tecnologie in collegamento con le Forze di polizia e gli Enti preposti;
- controllo del sistema informatico (cronologia, tempi, cookies, ecc.) da parte dei responsabili della manutenzione;

- installazione di *firewall* sull'accesso Internet;
- presenza di un docente durante l'utilizzo di Internet;
- aggiornamento periodico del software antivirus e scansione delle macchine in caso di sospetta presenza di virus;
- utilizzo di pen drive USB, CD-ROM e DVD o altri dispositivi esterni personali, solo se autorizzati e privi di virus.

Accesso alla rete

La scuola offre sia agli insegnanti sia agli alunni:

a) Postazioni LIM con collegamento ADSL alla rete;
b) Wi-Fi di istituto con accesso tramite password conosciuta solo dal personale docente;
c) Piattaforma di comunicazione e condivisione Scuola365

Relativamente agli alunni che accedono a Internet durante l'attività didattica, sono consentiti la navigazione guidata da parte dell'insegnante, la stesura di documenti collaborativi nonché l'utilizzo dei gruppi di discussione messi a disposizione da eventuali piattaforme didattiche, purché sotto il controllo dell'insegnante e nel caso in cui tale attività faccia parte di un progetto di lavoro precedentemente autorizzato.

Non è prevista la possibilità di crearsi account personali e scaricare la propria posta sui computer della scuola.

4. STRUMENTAZIONE PERSONALE

Per gli studenti: gestione degli strumenti personali (cellulari, tablet, ecc.)

Durante l'orario scolastico agli alunni non è permesso l'utilizzo della telefonia mobile in nessuna funzione.

A scuola è vietato l'uso per scopo personale di tutti gli altri strumenti informatici di proprietà dello studente.

L'eventuale utilizzo di strumenti informatici di proprietà dello studente durante una specifica attività didattica deve essere autorizzato dal Dirigente scolastico a seguito di richiesta del docente.

Le specifiche modalità di utilizzo concordate prevedono comunque la responsabilità e la vigilanza costante del docente stesso.

Per i docenti: gestione degli strumenti personali (cellulari, tablet, ecc.)

Per i docenti l'utilizzo di videofonini, di apparecchi per la registrazione di suoni e immagini è consentito esclusivamente per fini didattici (recite, video lezioni, attività progettuali…) e sempre nel

rispetto dei diritti e delle libertà fondamentali delle persone coinvolte, in particolare della loro immagine e dignità.

Non è possibile, in ogni caso, diffondere o comunicare sistematicamente i dati personali di altre persone (ad esempio immagini o registrazioni audio/video) senza aver prima informato adeguatamente le persone coinvolte e averne ottenuto l'esplicito consenso.

Stesse cautele vanno previste per l'uso dei tablet, se usati a fini di registrazione e non soltanto per fini didattici o per consultare in classe libri elettronici e testi on line.

Non violano la privacy le riprese video e le fotografie raccolte dai genitori durante le recite, le gite e i saggi scolastici. Le immagini in questi casi sono raccolte a fini personali e destinati ad un ambito familiare o amicale. Nel caso si intendesse pubblicarle e diffonderle in rete, anche sui social network, è necessario ottenere di regola il consenso delle persone presenti nei video o nelle foto.

5. PREVENZIONE, RILEVAZIONE E GESTIONE DEI CASI

Prevenzione

La sicurezza in Rete deve essere garantita come interesse pubblico, attraverso l'integrità delle infrastrutture e la loro tutela da attacchi, e come interesse delle singole persone (Art. 13, comma 1, Dichiarazione dei Diritti in Internet, 28 luglio 2015).

Rischi

La comunità scolastica può incontrare dei rischi a livello di contenuto, di contatto e di condotta:

Aree di rischio		
Contenuto	**Contatto**	**Condotta**
Esposizione a contenuti inappropriati. Visita di siti web inappropriati. Esposizione a siti che incoraggiano la violenza. Esposizione ad informazione la cui autenticità non è provata.	Grooming. Bullismo online in tutte le forme. Furto di identità.	Violazione della privacy e diffusione di informazioni personali. Reputazione online. Salute e benessere (intesa come quantità di tempo speso online per giochi e altro). Sexting (esibizione online di immagini intime). Violazione del copyright.

Azioni/Procedure: vedi compiti specifici figure di riferimento.
Protocolli di Intesa specifici saranno allegati non appena siglati.

Si segnala il percorso formativo relativo al progetto della Regione Lazio **"Piano di interventi ed azioni per la prevenzione, gestione e contrasto del fenomeno del bullismo e cyber-bullismo",** approvato con Determinazione Dirigenziale n. G15946, nell'ambito del quale la nostra Istituzione scolastica è risultata beneficiaria di fondi specifici, a fronte di presentazione di progetto dal titolo "Bullismo online e offline: in, out, oltre. Insieme.". Nel corso dell'a.s. 2017/18, le classi III-IV e V di scuola primaria e le classi I-II e III di scuola secondaria avranno l'opportunità di essere coinvolti in percorsi di formazione/informazione sulla tematica del bullismo e del cyber-bullismo; anche le Famiglie e i Docenti saranno coinvolti nella formazione a cura di formatori interni all'istituzione, delle Forze dell'Ordine (nell'ambito del progetto "Scuole sicure"), di psicologi (in qualità di supporto alla genitorialità). Per tutta la comunità scolastica, una campagna di sensibilizzazione ed informazione sulla cittadinanza digitale, intesa come media e social education.

Risultati progettuali attesi

per i ragazzi	-Educazione alla comunicazione e all'interazione e integrazione interpersonale -Conoscenza di Sé e dell' altro da Sé: presa di coscienza delle potenzialità contenute nelle diversità -uso consapevole dei social network, a cominciare dal discernimento sulla provenienza dei contenuti proposti - Riconoscimento immediato del fenomeno bullismo e cyberbullismo - Individuazione di strategie singole e di gruppo per fronteggiare il problema - conoscenza e comprensione dei ruoli insiti nel bullismo e nel cyberbullismo: delle vittime, dei carnefici, degli spettatori
Per le famiglie	- Educazione all' ascolto, all'empatia e alla condivisione: educazione alla genitorialità - Educazione alla percezione dei segni rivelatori del fenomeno bullismo e cyberbullismo - Conoscenza delle potenzialità e dei pericoli del web - Conoscenza delle possibili strategie di intervento in caso di episodi di bullismo e cyberbullismo: limite tra libertà e responsabilità in rete
Per il personale scolastico e altre agenzie formative	Formazione più diffusa su: - Educazione alla percezione dei segni rivelatori del fenomeno bullismo e cyberbullismo - Conoscenza approfondita delle potenzialità e dei pericoli del web e di strategie di intervento appropriate - Maturazione di abilità assertive utili a fronteggiare il problema
Per il territorio	Diffusione di una maggiore consapevolezza del fenomeno del bullismo e del cyber bullismo e di strumenti per la prevenzione, l'individuazione e la presa in carico delle situazioni.