Liceo Scientifico-Musicale-Sportivo
Attilio Bertolucci

DOCUMENTO DI E-POLICY

1. PREMESSA

La presenza sempre più capillare delle nuove tecnologie nella vita quotidiana di ognuno ha inevitabilmente interessato la scuola nelle sue multiformi realtà. In particolare, lo sviluppo e l'integrazione del loro uso nella didattica interroga chi ha responsabilità educative nel uso sicuro e consapevole.

Il nostro istituto, scuola 2.0 fin dai suoi primi anni di vita, ha quindi da sempre manifestato e dichiarato la sua vocazione all'integrazione delle nuove tecnologie con la didattica, supportata dagli evidenti benefici nel processi di insegnamento/apprendimento.

Il Liceo "Attilio Bertolucci" sostiene l'uso della tecnologia allo scopo di accrescere e sostenere l'apprendimento e offre agli studenti accesso alle reti informatiche affinché possano avvalersi della tecnologia in qualsiasi momento del giorno.

Uno degli obiettivi tecnologici della scuola è garantire che l'interazione di ogni utente con la tecnologia contribuisca positivamente all'ambiente educativo a scuola.

In quest'ottica, occorre condurre gli studenti nella crescita sull'uso corretto delle nuove tecnologie.

A tal proposito, il Garante della Privacy è intervenuto negli scorsi anni col documento "La scuola a prova di privacy" e con dispositivi più recenti per quello che riguarda la protezione dei dati personali.

Da tempo il nostro liceo si è dimostrato attivo nello studio, analisi e confronto di tematiche e rischi legati all'uso delle nuove tecnologie: la partecipazione a corsi di perfezionamento, la rilevazione interna di dati sull'utilizzo dei dispositivi, la collaborazione con "Generazioni Connesse", la partecipazione ad incontri di formazione, incontri con i genitori degli alunni, l'emanazione di norme interne riguardo l'uso ed abuso dei dispositivi informatici (Regolamento di istituto; il Patto di corresponsabilità (sottoscritto da genitori e studenti); l'Accordo per l'utilizzo dei dispositivi personali (BYOD)), informativa sul trattamento dei dati personali (ai sensi dell'art. 13 del D. Lgs. 30 giugno 2003, n. 196, e richiesta di autorizzazione all'utilizzo dei dati personali degli alunni eccedenti i trattamenti istituzionali obbligatori, come per esempio l'utilizzo di fotografie, video o altri materiali audiovisivi contenenti l'immagine, il nome e/o la voce del proprio figlio/a, all'interno di attività educative e didattiche per scopi documentativi, formativi e informativi, durante gli anni di frequenza della scuola), ecc.

Il rispetto delle regole contenute nei citati documenti, viene rammentato all'inizio di ogni anno scolastico tramite una circolare diffusa a tutto il personale scolastico nonché agli studenti ed alle loro famiglie, che prevede le modalità di utilizzo dei dispositivi personali all'interno dell'istituto.

La redazione del presente documento nasce dalla necessità di dare concretezza alle "Linee di orientamento" emanate nell'aprile 2015 tenendo conto, altresì, dei recenti interventi normativi e, in particolare, delle novità contenute nella L.71/2017 "Disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del cyberbullismo".

Come, invero, precisato dalle citate Linee di orientamento *"…con l'evolversi delle tecnologie, l'espansione della comunicazione elettronica e on-line e la sua diffusione tra adolescenti e pre-adolescenti, il bullismo ha assunto le forme subdole e pericolose del cyberbullismo che richiedono la messa a punto di nuovi e più efficaci strumenti di contrasto…".*

Lo scopo che ci si propone in questa sede è, dunque, quello di descrivere l'approccio dell'istituto alle tematiche legate alle competenze digitali, all'uso degli stessi in ambiente scolastico, ed alla sicurezza in rete in termini di:

- ✓ individuazione di norme comportamentali e delle procedure per l'utilizzo delle **Tecnologie dell'Informazione e della Comunicazione (TIC)**;
- ✓ promozione dell'uso positivo delle tecnologie digitali nella didattica;
- ✓ adozione delle misure per la prevenzione del fenomeno del cyberbullismo e, contestualmente, individuazione degli strumenti di tutela per chi risultasse vittima di

comportamenti (anche solo potenzialmente) vessatori e di emarginazione attraverso un uso distorto e violento della rete;

- ✓ sensibilizzazione degli studenti, orientandoli verso un uso corretto delle tecnologie digitali.

Il tutto in coerenza con lo spirito della Legge 71/2017 che è quello di un approccio sostanzialmente inclusivo, con interventi dalla finalità educativa e mai punitiva.

Il presente documento sarà soggetto a revisioni ed aggiornamenti periodici e sottoposto all'attenzione dei competenti Organi Collegiali.

2. STRUMENTAZIONE TIC DELLA SCUOLA – DIDATTICA E FORMAZIONE

Ogni aula della scuola è dotata di almeno una postazione PC e di una LIM. Esiste, inoltre, un laboratorio di informatica con postazioni fisse nonché una serie di dispositivi informatici mobili (tablet, PC portatili, routers mobili), con relativo carrello di ricarica.

L'accesso alla rete attraverso il server d'istituto e l'intera copertura wifi della scuola, è, inoltre, controllato da un *software Firewall* che funge da filtro impedendo l'uso scorretto della rete.

L'istituto inoltre ha un proprio sito costantemente aggiornato, che prevede l'accesso al registro elettronico, alle diverse sezioni dell'istituto, ai principali documenti pubblici, ecc.

Per la salvaguardia dei diritti d'autore, il liceo si è da tempo dotato di software antiplagio che consente il controllo informatico sulla rete dei lavori degli studenti.

Il "Bertolucci" gestisce anche un proprio Blog ed un proprio Magazine sulle iniziative e sulla vita della scuola.

Collabora con l'agenzia DIRE di Roma per la produzione di materiale relativo agli usi impropri della rete e dei dispositivi, in collaborazione con Generazioni Connesse.

In coerenza con il Piano Nazionale Scuola Digitale (PNSD) agli studenti è inoltre consentito l'uso di dispositivi personali con finalità didattico-educative nel rispetto del presente documento e dell'accordo BYOD firmato anche dai genitori (BYOD – Bring Your Own Device). I ragazzi, infatti, sotto la guida ed il controllo costante del docente, possono accedere alla rete utilizzando direttamente il proprio dispositivo in classe per approfondire ed implementare le proprie conoscenze. Il che impone, a maggior ragione, la necessità di educarli sul tema della sicurezza in rete nonché sull'uso corretto e responsabile delle tecnologie digitali.

In proposito, è già stato oggetto di approvazione ed è, pertanto, attualmente in vigore un sistema di regole per il corretto utilizzo dei dispositivi personali (BYOD Policy - accordo

per l'utilizzo dei dispositivi personali, Regolamento di Istituto, decalogo del Garante sulla Privacy, ecc.).

Proprio in considerazione dei mutati obiettivi della didattica, maggiormente orientati all'acquisizione di competenze (in particolare quelle digitali oggi annoverate tra i saperi necessari nell'ambito della cittadinanza digitale, in termini di: elaborazione delle informazioni, comunicazione, creazione di contenuti, sicurezza e risoluzione di problemi), particolare importanza dovrà essere attribuita anche alla formazione dei docenti sulle tematiche della sicurezza, aderendo alle iniziative che saranno ritenute idonee allo scopo.

3. VALUTAZIONE DEI RISCHI

L'uso di internet e delle nuove tecnologie è diventato sempre più precoce, frequente ed intenso per le nuove generazioni, che si ritrovano quindi ad affrontare dinamiche specifiche dei nuovi ambienti in rete, legate all'identità, alle relazioni, alla privacy, alla reputazione, alla produzione, distribuzione e fruizione di contenuti. Peraltro, recenti ricerche (EU kids online) hanno mostrato che all'aumentare delle opportunità aumentano anche i rischi, suggerendo quindi di lavorare a strategie di mediazione e prevenzione per un uso consapevole, corretto e creativo.

Nella valutazione dei possibili rischi, oltre a considerare le minacce provenienti dall'esterno rispetto al contesto scolastico, si ritiene opportuno non sottovalutare la possibilità che ad agire in modo illecito, provocando i danni più seri, siano spesso proprio quei soggetti che operano dall'interno e che, pertanto, conoscono la struttura della rete in qualità di fruitori dei servizi.

Ciò posto, i principali rischi connessi all'uso delle tecnologie digitali risultano essere:

- la possibile dipendenza (patologica) dalla rete (social network, gambling, vamping, ecc.);
- l'uso improprio e scorretto dei dati personali (furto di identità – frode con carte di credito);
- episodi di cyberbullismo;
- esposizione a filmati violenti o a contenuto pedopornografico;
- relazioni pericolose/adescamento in rete;
- incitazione all'odio;
- persuasori con finalità commerciali;
- divulgazione di notizie false;

- uso della rete per giudicare, infastidire o impedire a qualcuno di esprimersi o partecipare.

4. RUOLI E RESPONSABILITÀ

La pervasività delle nuove tecnologie nella vita personale, i rischi ad esse connesse, le sue potenzialità e l'esponenziale crescita dei contatti e delle relazioni, pone spesso il singolo di fronte ad una duplice situazione da vivere: la realtà "concreta" e quella virtuale, tra loro oramai fortemente connesse, influenzate e spesso determinate. La nascita poi di gruppi in rete richiedono capacità comunicative e socio-relazionali adeguate.

È fondamentale quindi conoscere come comportarsi in questi gruppi, quali regole vanno rispettate e quali ruoli e responsabilità hanno i soggetti che vi partecipano.

È opportuno quindi che anche nell'ambito scolastico ci sia chiarezza sui ruoli e sulle responsabilità di ciascun attore del percorso formativo.

- Il **Dirigente scolastico** è il soggetto su cui incombe la responsabilità di garantire la sicurezza dei membri della comunità scolastica e, conseguentemente, anche della sicurezza in rete. In quest'ottica egli si preoccupa di:
  - ✓ 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;
  - ✓ dotare la scuola di un sistema in grado di consentire il controllo della sicurezza in rete;
  - ✓ seguire le procedure relative agli eventi dannosi eventualmente occorsi agli alunni nell'utilizzo delle TIC a scuola.

- L'**Animatore digitale** si preoccupa di:
  - ✓ promuovere 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 minute problematiche;
  - ✓ rilevare le criticità proponendo soluzioni adeguate e sostenibili;

- ✓ interessarsi dell'aggiornamento delle politiche di istituto sulla della rete della scuola, e nella proposta di novità ed aggiornamento metodologico e tecnologico implementabile nella rete di istituto ad uso di tutto il personale scolastico;
- ✓ gestire e controllare l'accesso alla rete ed ai servizi di istituto (posta elettronica, G-suite, ecc.) da parte degli utenti mediante credenziali personalizzate, firewall, antivirus, ecc.
- ✓ individuare progetti ed attività aventi ad oggetto la sicurezza in rete in cui coinvolgere la comunità scolastica (alunni, genitori, docenti).

- Il **Direttore dei Servizi Generali e Amministrativi** deve:
  - ✓ assicurare, 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;
  - ✓ garantire la comunicazione all'interno dell'istituto, tra la rete di scuole (sportello, circolari, sito web, ecc.), e fra la scuola e le famiglie degli alunni per la diffusione di informazioni nell'ambito dell'utilizzo delle tecnologie digitali e della rete.

- I **docenti** si impegnano a:
  - ✓ informarsi e ad aggiornarsi su tema della sicurezza in rete uniformandosi alle politiche di sicurezza adottate dalla scuola di cui rispettano il regolamento;
  - ✓ 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.);
  - ✓ guidare gli studenti nella scelta della fonte di informazioni;
  - ✓ 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.

- Agli **alunni** è richiesto di:
  - ✓ 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.

- Anche i **genitori** sono coinvolti a pieno titolo. Ad essi è richiesto 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 digitali.

5. DISPOSITIVI PERSONALI

5.1 STUDENTI

Gli alunni possono portare il dispositivo (smartphone) a scuola. Secondo con quanto indicato dalla Direttiva Ministeriale n. 30 del 15 marzo 2007, dall'accordo BYOD POLICY, e dal Garante sulla Privacy, gli studenti devono a tenere il dispositivo (smartphone) **spento** quando sono a scuola, indipendentemente dall'attività svolta (lezione, ricreazione, accesso ai servizi igienici, pause, ecc.).

Tuttavia, se il docente lo ritiene opportuno, è consentito l'uso del dispositivo personale dello studente che quindi utilizzerà esclusivamente la rete scolastica. Si recepisce in questo documento quanto previsto dalla Direttiva Ministeriale n. 30 del 15 marzo 2007: "le famiglie si assumono l'impegno di rispondere direttamente dell'operato dei propri figli nel caso in cui, ad esempio, gli stessi arrechino danni ad altre persone".

5.2 DOCENTI

Non è consentito l'uso del dispositivo (smartphone) durante le ore di lezione. È consentito l'uso di altri dispositivi elettronici personali solo a scopo didattico ed integrativo di quelli scolastici disponibili. Per il restante orario di servizio è consentito l'uso del dispositivo (smartphone) solo per importanti comunicazioni personali urgenti.

5.3 PERSONALE DELLA SCUOLA

Il personale scolastico è autorizzato ad usare il proprio dispositivo se non sta svolgendo un ruolo didattico, solo se l'utilizzo non intralci il normale svolgimento delle attività scolastiche, né distragga dal corretto svolgimento delle proprie mansioni.

6. MODALITÀ DI SEGNALAZIONE DI SITUAZIONI E/O COMPORTAMENTI A RISCHIO

Qualora il personale scolastico, non solo la figura docente, dovesse rilevare possibili situazioni di disagio connesse ad uno o più di uno tra i rischi elencati precedentemente, dovrà compilare uno dei moduli di segnalazione del presente documento, e informare il dirigente scolastico, ovvero il docente coordinatore di classe.

Il dirigente scolastico contatterà il docente e/o il personale scolastico per un colloquio finalizzato all'analisi della situazione ed alle azioni da intraprendere. Ove necessario, si coinvolgerà la famiglia.

7. OPERAZIONI RELATIVE AL MANCATO RISPETTO DELLA E-POLICY

Nell'ambito delle responsabilità del D.S.G.A., dell'animatore digitale e dei docenti, si fa riferimento alle funzioni di responsabilità e controllo dirigenziale.

Il personale scolastico è tenuto a collaborare col D.S. per fornire ogni informazione utile per le valutazioni del caso e per l'avvio di eventuali procedimenti organizzativo-gestionale, disciplinare, amministrativo, civile, penale, ecc.

Si chiede, inoltre, anche ai genitori di farsi carico della propria parte, in quanto principale figura educativa dei propri figli. A seguito di una rilevazione interna all'istituto effettuata due anni addietro, si segnalano alcune situazioni di criticità degli studenti in ambito domestico cui si chiede alla famiglia di prestare attenzione:

- una totale autonomia nella navigazione sul web e nell'utilizzo dello smartphone;
- ricorso ad ambienti della casa dove è minore o assente il controllo parentale;

- la piena e totale disponibilità a qualsiasi ora del giorno o della notte del proprio dispositivo mobile;
- un utilizzo del dispositivo che non consenta la memorizzazione di siti e/o materiali non idonei.

Le principali operazioni relative al mancato rispetto della E-policy da parte degli alunni sono riconducibili a:

- uso di social network e blog per pubblicare, condividere o, in genere, postare commenti o giudizi offensivi della dignità altrui;
- condivisione di dati personali che possano permettere l'identificazione;
- connessioni a siti proibiti o comunque non autorizzati;
- pirateria informatica;
- scaricamento di file (video, film, musica, immagini, test, ecc.) per finalità personali;
- pubblicazione di foto o immagini non autorizzate e/o compromettenti.

Gli interventi previsti sono rapportati all'età, alla situazione personale, alla gravità dell'operato. Si riporta di seguito un elenco non esaustivo di possibili azioni:

- richiamo verbale;
- richiamo verbale con annotazione disciplinare sul registro e/o sul diario personale;
- prelievo del dispositivo e consegna all'ufficio alunni per il ritiro dello stesso da parte dei genitori;
- convocazione della famiglia e/o degli attori dell'episodio segnalato;
- raccolta del materiale informatico lesivo della dignità delle figure presenti nell'istituto;
- sanzione disciplinare grave;
- accesso alla commissione di garanzia;
- segnalazione alle forze dell'ordine.

Le figure interessate alla definizione dell'azione da intraprendere sono le seguenti, in ordine di gravità:

- personale scolastico / docente verso il coordinatore di classe (bassa entità);
- personale scolastico / docente verso consiglio di classe ed eventuale coinvolgimento della famiglia (media entità);
- personale scolastico / docente verso consiglio di classe, dirigente scolastico e coinvolgimento della famiglia (entità grave);

- personale scolastico / docente verso dirigente scolastico, coinvolgimento della famiglia ed agenti esterni quale le forze dell'ordine e/o la polizia postale (entità gravissima).

La Legge 71/2017, nell'articolo 2, cui si rimanda, indica tempi e modalità per richiedere la rimozione di contenuti ritenuti dannosi per i minori.

La Legge 71/2017, agli articoli 5 e 7, cui si rimanda, riporta due sanzioni nei confronti dei trasgressori della legge stessa, minorenni e di età superiore ai quattordici anni (rispettivamente sanzioni disciplinari in ambito scolastico con percorsi di recupero, ammonimento con la famiglia presso il questore).

La scuola potrà, altresì, segnalare episodi di cyberbullismo nonché la eventuale presenza di materiale pedopornografico in rete al servizio Helpline di Telefono Azzurro 1.96.96, alla Hotline "Stop-it" di Save the Children, all'indirizzo www.stop-it.it affinché trasmettano dette segnalazioni al Centro Nazionale per il Contrasto alla Pedopornografia su Internet, istituito presso la Polizia Postale e delle Comunicazioni, per consentire le attività di investigazione necessarie.

Le azioni individuate hanno la finalità di sostenere le vittime, le famiglie e tutti coloro che sono stati spettatori attivi o passivi di quanto avvenuto, e di realizzare interventi educativi nei confronti di coloro che hanno messo in atto comportamenti lesivi del rispetto degli altri.

In ogni caso, i docenti predisporranno specifiche rilevazioni ed azioni preventive sulla base dei protocolli suggeriti dalla piattaforma "Generazioni Connesse", e dei percorsi formativi anche in rete. A tal fine, sono stati predisposti dei moduli ad hoc reperibili sul loro sito, che costituiscono parte integrante del presente documento.

8. MODULI DI SEGNALAZIONE

Si riporta di seguito la scheda per la rilevazione della violazione delle disposizioni sull'uso della strumentazione personale, e quella di segnalazione di casi connessi ai rischi della rete.

[*documento approvato dal collegio docenti – 16 maggio 2018*]

SCHEDA PER LA RILEVAZIONE DI VIOLAZIONE DELLE DISPOSIZIONI SULL'USO DELLA STRUMENTAZIONE PERSONALE

ALUNNO:			
CLASSE:		**SEZIONE:**	
PLESSO:		**ORDINE DI SCUOLA:**	

DOCENTE/I COINVOLTI	
DATA DELLA VIOLAZIONE	
DESCRIZIONE DEI FATTI	

Firme Docenti coinvolti

_____ _____

_____ _____

SCHEDA DI SEGNALAZIONE

ALUNNO:			
CLASSE:		**SEZIONE:**	
PLESSO:		**ORDINE DI SCUOLA:**	

NOTIZIE SULLA STORIA SCOLASTICA PRECEDENTE:

RAPPORTI CON LA FAMIGLIA:

PROBLEMI EVIDENZIATI

OSSERVAZIONE DIRETTA	EVENTO RIFERITO	DESCRIZIONE
		Esposizione a contenuti violenti
		Uso di videogiochi diseducativi
		Accesso ed utilizzo di informazioni scorrette o pericolose
		Scoperta ed utilizzo di virus in grado di infettare computer
		Possibile adescamento
		Cyberbullismo (rischio di molestie o maltrattamenti da coetanei)
		Sexting (scambio di materiale a sfondo sessuale)
		Dipendenza da uso eccessivo
		Divulgazione di notizie false
		Incitazione all'odio
		Uso improprio e scorretto dei dati personali

Firme Docenti coinvolti

_____ _____

_____ _____