PUA - Politiche d'Uso Accettabile e Sicuro della Rete

Per un uso consapevole, corretto e sicuro delle Tecnologie dell'Informazione e della Comunicazione (TIC) nella didattica.

Gruppo PNSD

Liceo E.Q. Visconti - Roma - a.s. 2017-2018

SOMMARIO

1 Premessa e finalità

Il Liceo classico Ennio Quirino Visconti (nel seguito *Istituto*), visto il crescente utilizzo di internet e delle Tecnologie dell'informazione e della comunicazione (nel seguito TIC) nella scuola, vista la normativa vigente a riguardo, sentito il parere del Collegio dei Docenti, stabilisce con il presente documento, le politiche d'uso accettabile e sicuro della rete, delle TIC nell'*Istituto*.

Il presente documento ed i documenti ad esso correlati sono stati approvati dal Consiglio d'Istituto in data _____ .

Scopo del presente documento sulla politica per un uso accettabile e sicuro della rete (nel seguito PUA) è quello di informare l'utenza e coloro che operano nell'*Istituto* al fine di garantire un uso attento, corretto e responsabile di internet e delle TIC nel rispetto della normativa vigente, della comunità scolastica e della salvaguardia dei beni comuni.

Il presente documento, pertanto, ha carattere generale e si rivolge a tutta la comunità scolastica dell'*Istituto*: studenti, genitori, docenti, personale ATA; ad esso sono collegati i seguenti documenti di riferimento normativo presenti nella sezione "Normative e sicurezza" del sito d'*Istituto*:

- Regolamenti
  - Regolamento del laboratorio d'informatica
  - Regolamento d'uso di G Suite for Education, nelle due versioni (Regolamento Docente/Regolamento Studente)
- Normative
  - Codice comportamentale MIUR 28/11/2016
  - D Lgs.196/2003
  - Regolamento Unione Europea 2016/679
  - Normativa privacy- vademecum aggiornato http://liceoeqvisconti.gov.it/index.php/normative-e-sicurezza/privacy
  - MIUR Piano nazionale per l'educazione al rispetto, Linee Guida Nazionali (art. 1 comma 16 L. 107/2015) e Linee di orientamento per la prevenzione e il contrasto del cyberbullismo nelle scuole (art. 4 L. 71/2017) http://www.noisiamopari.it/site/it/home-page/
  - MIUR Basta bufale - Campagna contro le fake news - http://www.generazioniconnesse.it/site/it/fake-news/
  - Dichiarazione dei Diritti in Internet - Testo legislativo (L. 71/2017 ; Nota MIUR Prot.5515 del 27/10/2017)
  - Linee di orientamento prevenzione e contrasto - Bullismo e Cyberbullismo - MIUR
  - Linee di orientamento del MIUR contro il cyber-bullismo
- Sicurezza informatica:
  - Social privacy - Come tutelarsi nell'era dei social network http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3140082
  - SICUREZZA INFORMATICA - Firewall e Web Filtering

http://liceoeqvisconti.gov.it/index.php/normative-e-sicurezza/norme-sulla-sicurezza

- Della predisposizione del PUA viene data specifica informativa a tutta la comunità scolastica, che è tenuta al rispetto del presente documento PUA e di tutti i documenti ad esso correlati precedentemente indicati.

Tutto il personale dell'Istituto, docente e ATA è tenuto al rispetto del presente PUA, rispondendo dei propri comportamenti, ciascuno nello specifico ambito delle proprie competenze. Il documento integrale è disponibile nel sito dell'*Istituto* nella sezione "Normative e sicurezza".

2 I vantaggi della rete e delle TIC nella scuola

Partendo dalla constatazione che le TIC sono la "nuova lingua" del terzo millennio e che i giovani risultano "nativi" del mondo digitale, è urgente cercare di avvicinare il più possibile il mondo della scuola a quello delle nuove tecnologie, fornendo agli studenti una educazione e una formazione per un uso critico, consapevole e costruttivo dei potenti strumenti che quotidianamente utilizzano.

Il curricolo scolastico infatti prevede che gli studenti imparino a trovare materiale, consultare documenti e scambiare informazioni utilizzando le TIC.

L'*Istituto* propone agli studenti e ai docenti di utilizzare Internet per promuovere le competenze culturali e di cittadinanza in ambito didattico attraverso la condivisione delle risorse, l'innovazione e la comunicazione.

Le TIC a scuola rappresentano l'occasione per creare un nuovo ambiente di apprendimento in cui gli studenti possono trovare nuove opportunità per lavorare insieme, per studiare in modo creativo e autonomo, svolgere esercitazioni, ricercare informazioni, comunicare, consolidare le nozioni apprese e diventare non solo fruitori ma anche autori di prodotti multimediali. La rete internet e le connesse forme di comunicazione offrono occasioni di sviluppo espressivo di se stessi e della propria identità, offrono canali e spazi in cui potersi relazionare con altre persone, anche fisicamente molto lontane, entrando in contatto con culture e paesi differenti.

In questo modo l'apprendimento può diventare più semplice, più "fluido" ed efficace. Gli studenti, se adeguatamente accompagnati e formati, possono trarre maggiori motivazioni all'apprendimento attraverso un incremento della curiosità, sviluppando un senso critico nel discernere e nell'orientarsi all'interno della sconfinata quantità di informazioni presenti in rete.

Per gli studenti e per i docenti l'accesso ad Internet è quindi uno strumento didattico e, poiché esiste la possibilità che gli studenti trovino materiale inadeguato e illegale su Internet, l'*Istituto* ha assunto precauzioni limitando opportunamente l'accesso ad Internet.

I docenti hanno la responsabilità di guidare gli studenti nelle attività online, di stabilire obiettivi chiari nell'uso di Internet, insegnando un uso della rete accettabile e responsabile.

Le nuove tecnologie si presentano come uno strumento efficace per la contestualizzazione degli argomenti, la realizzazione di esperienze significative di apprendimento, la riflessione e il consolidamento delle conoscenze acquisite e l'applicazione pratica e dinamica di quanto appreso.

Non va inoltre dimenticato che la "competenza digitale" è inclusa tra le otto competenze chiave (cioè quelle di cui tutti necessitano per la realizzazione e lo sviluppo personali, per la cittadinanza attiva, per una piena inclusione sociale e per l'occupazione) da assicurare nei percorsi formativi di tutti i cittadini europei secondo le raccomandazioni delle istituzioni comunitarie (Consiglio dell'Unione Europea e Parlamento Europeo - 18 dicembre 2006 - 2006/962/CE).

L'obbiettivo principale dell'utilizzo consapevole, corretto e sicuro di internet e delle TIC nella scuola rimane quello di contribuire a:

- migliorare l'apprendimento degli studenti;
- arricchire la didattica curriculare in aula;
- integrare nel lavoro didattico svolto in aula i vari strumenti tecnologici (LIM, tablet, ecc...);
- stimolare negli studenti e nei docenti un atteggiamento positivo e attivo verso la tecnologia;
- offrire valore aggiunto e risorse agli studenti.

Le nuove tecnologie, inoltre, possono costituire un valido strumento di ausilio per gli studenti in situazione di svantaggio e/o con disturbi di apprendimento, elevando la soglia di attenzione e di interazione e permettendo un più proficuo recupero degli apprendimenti.

3 Stato di fatto

Le TIC impiegate nell'*Istituto* sono utilizzate da una serie di utenti in un certo numero di spazi sia fisici che virtuali attraverso una serie di dispositivi dell'*Istituto* o di proprietà degli utenti.

Gli utenti delle TIC appartengono alle seguenti categorie:

- Studenti;
- Genitori;
- Docenti;
- Personale ATA.

Gli spazi fisici sono i seguenti:

- Aule;
- Laboratori;
- Aula Professori / Biblioteca;
- Sala Magna;
- Uffici amministrativi;
- Aree comuni.

Gli spazi virtuali sono quelle aree informatiche a cui si accede attraverso un processo di autenticazione che utilizza:

- un dispositivo informatico dell'*Istituto* o personale,
- una chiave d'accesso fornita dall'*Istituto* (se necessario).

Gli spazi virtuali messi a disposizione dell'utenza dall'*Istituto* sono:

- la rete WiFi;
- la rete LAN;
- l'accesso sicuro ad Internet attraverso un sistema di filtraggio del traffico dati (Firewall);
- le aree di archiviazione sui PC dell'*Istituto;*
- il sito dell'Istituto ed i siti collegati;
- il registro elettronico Argo;
- i servizi di G Suite for Education di Google (Posta Elettronica, Google Drive, ecc…).

I dispositivi dell'Istituto per le TIC negli spazi fisici dell'*Istituto* sono i seguenti:

- nelle aule:
  PC, LIM, Casse Acustiche, Tablet del Docente;
- nei laboratori:
  PC Docente, Proiettore, Impianto acustico, solo nel laboratorio d'informatica PC Postazioni studenti;
- nell'aula magna:
  PC, Proiettore, Microfono e Impianto acustico;
- nell'aula professori / Biblioteca;
  PC per Docenti, PC Biblioteca, Stampante di rete;
- negli uffici amministrativi:
  PC postazioni personale amministrativo, Server di rete per archiviazione documenti, Stampanti in rete;
- nelle aree comuni:
  solo per i docenti e il personale ATA, rete WiFi e fotocopiatrici;

Le chiavi di accesso agli spazi virtuali sono:

- chiave di accesso alla rete WiFi:
  solo per i docenti, è impostata una volta per tutte sul dispositivo tablet assegnato al docente dall'*Istituto* e/o sul proprio dispositivo personale per accedere alla rete d'I*stituto* in presenza;
- chiave di accesso ad Internet:
  ai docenti è assegnata la chiave di accesso ad internet che deve essere utilizzata per navigare su internet attraverso la rete d'*Istituto.*
  Agli studenti è assegnata una chiave di accesso ad internet quando devono navigare utilizzando i PC del laboratorio d'informatica, questa chiave ha una scadenza temporale.
- chiave di accesso al registro elettronico:
  tutta la comunità scolastica dell'Istituto può accedere ai servizi del registro elettronico Argo attraverso una chiave che identifica il singolo utente nel proprio ruolo di studente, genitore, membro del personale docente o amministrativo.
- chiave di accesso a G Suite for Education:
  ai docenti ed agli studenti è assegnata una chiave di accesso a G Suite for education per utilizzare i servizi messi a disposizione da Google attraverso la piattaforma G Suite, ed in particolare la posta elettronica, lo spazio di archiviazione G DRIVE, ed altri servizi secondo quanto stabilito dai Regolamenti d'utilizzo di G Suite for Education.
- chiave di accesso ai PC dell'Istituto:

è una chiave senza password, quindi non personale, che consente di utilizzare le risorse informatiche di ogni PC dell'Istituto, ad esempio consente di archiviare documenti sui dispositivi di archiviazione dei PC oppure permette di visualizzare filmati, utilizzare la LIM nelle aule, ecc…

- chiave di accesso al sito dell'*Istituto*:
  il sito dell'Istituto è pubblico, non necessita di chiavi di accesso, le aree riservate del sito sono accessibili attraverso chiavi di accesso già definite in precedenza.

4 Valutazione dei rischi

L'*Istituto* si fa carico delle precauzioni necessarie e possibili per assicurare agli studenti l'accesso a materiale appropriato, anche se risulta impossibile evitare in modo assoluto che gli studenti trovino materiale indesiderato navigando in rete attraverso uno degli spazi virtuali messi a disposizione. L'*Istituto* pertanto non può farsi carico della responsabilità per il materiale trovato su internet o per eventuali conseguenze causate dalla navigazione o da un uso irresponsabile e scorretto degli strumenti tecnologici.

Gli studenti apprenderanno come utilizzare corretti metodi e strumenti di ricerca su internet e come giovarsi del servizio di posta elettronica e degli altri strumenti di comunicazione sotto la guida e la vigilanza dei docenti. L'utilizzo dei dispositivi informatici da parte degli studenti è vietato senza autorizzazione del docente.

Gli studenti devono essere pienamente coscienti dei potenziali rischi a cui si espongono navigando in rete e devono pertanto essere educati a riconoscere gli aspetti negativi e/o illeciti di internet come la pornografia, il razzismo, la violenza, lo sfruttamento dei minori ed ogni forma di istigazione ad essi connessa. Agli studenti non dove essere sottoposto materiale di questo tipo e se ne venissero a contatto devono sempre ed immediatamente segnalarne l'indirizzo internet (URL) al docente o al responsabile tecnico delle TIC (anche allo scopo di prevedere un affinamento del filtraggio).

4.1 Rischi esterni

I principali rischi esterni indotti dalla presenza nell'*Istituto* di collegamenti alla rete internet e all'utilizzo delle TIC sono:

- accessi non desiderati:
  le postazioni di lavoro e i dati in esse contenuti possono essere manomessi, manipolati, sottratti o alterati da accessi alla rete interna da parte di soggetti estranei e non autorizzati (hacker/cracker);
- virus:
  la navigazione internet, il download di files, la condivisione di materiale e l'utilizzo della posta elettronica possono essere dei potenziali veicoli di trasmissione di virus informatici e/o trojan. I rischi consistono nella perdita di dati, dell'accesso agli stessi da parte di soggetti non autorizzati, il danneggiamento dei PC con conseguenti malfunzionamenti o rallentamenti.
- email spamming:

nonostante le caselle di posta dell'*Istituto* si appoggino su server Google, che fornisce un servizio "a monte" di antivirus e di antispam, e nonostante l'*Istituto* sia protetto da un sistema di Firewall per il filtraggio del traffico dati in entrata/uscita, tuttavia può verificarsi, soprattutto nell'utilizzo di caselle email personali, la ricezione o l'inavvertito inoltro di email false non richieste e non sollecitate, con conseguenti problemi di accesso non desiderato, malfunzionamenti e sovraccarico delle applicazioni e dei dispositivi.

- intercettazione dei dati
- denial of Service (DOS):
  è possibile che, in seguito a manomissioni o alterazioni o malfunzionamenti, un servizio possa essere temporaneamente non disponibile agli utenti, fino al caso più grave di completa manomissione.

4.2 Rischi interni

I principali rischi interni indotti dalla presenza nell'*Istituto* di collegamenti alla rete internet e all'utilizzo delle TIC sono:

- utilizzo degli spazi virtuali, rete o altro, da parte di utenti non autorizzati all'accesso;
- intrusioni in spazi virtuali da parte di utenti non autorizzati e violazioni delle restrizioni e dei controlli stabiliti;
- trasmissione illecita di dati attraverso internet da parte di chi ha ottenuto accesso a dati (anche sensibili o riservati) verso soggetti non autorizzati a ricevere/manipolare tali dati;
- navigazione su siti internet con contenuti illeciti, offensivi e/o comunque non pertinenti con l'attività dell'*Istituto*, nonostante la navigazione sia sottoposta a filtraggio;
- traffico non consentito: la navigazione su internet può interferire pesantemente con le attività istituzionali in quanto lo scaricamento e lo scambio di immagini, file multimediali (audio e video) e "app" può comportare un inevitabile sovraccarico di rete. Occorre quindi che tutti gli utenti pongano attenzione al sovraccarico della rete dell'*Istituto* nelle diverse attività svolte;
- manomissioni, danneggiamenti di sistemi, firewall e apertura di back-door. In questo caso si provvede immediatamente alla revoca di tutte le autorizzazioni, provvedendo alla generazione di nuovi account.

5 Strategie adottate dall'Istituto per la sicurezza delle TIC

Nonostante l'*Istituto* provveda a mettere in atto tutte le misure ritenute necessarie al fine di raggiungere una adeguata sicurezza relativamente alle TIC, occorre sottolineare come la consapevolezza dei rischi che si corrono con l'utilizzo della rete e delle nuove tecnologie è un problema di tipo culturale ed educativo e deve essere ottenuta soprattutto attraverso la sensibilizzazione ed il coinvolgimento attivo di tutti gli utenti, insieme ad una corretta organizzazione di prodotti e processi.
Le strategie previste dall'*Istituto* per la sicurezza in rete sono le seguenti:

- accesso alla rete internet identificato tramite username e password, per una sessione di lavoro con scadenza temporale (sessione rinnovabile);
- accesso con password alla rete wi-fi;
- uso di un sistema di Web Content Filtering, configurato in modo da impedire nella navigazione in internet l'accesso a siti ritenuti inopportuni per i minori (es. pornografia,

violenza, razzismo, giochi online...) per evitare che vengano visualizzati siti web inappropriati. Le regole di filtraggio (policy per l'uso sicuro) possono essere implementate tramite software a livello di rete (vedi documento "SICUREZZA INFORMATICA – Firewall e Web Filtering);

- utilizzo di un firewall fisico per impedire l'accesso dall'esterno ai computer della scuola e prevenire attacchi combinati o utilizzi non autorizzati finalizzati a bloccare le attività dell'*Istituto* (vedi documento "SICUREZZA INFORMATICA – Firewall e Web Filtering);
- aggiornamento periodico del software antivirus, del firewall e scansione delle macchine in caso di sospetta presenza di virus (vedi documento "SICUREZZA INFORMATICA – Firewall e Web Filtering);
- limitatamente a ciò che riguarda la sfera lavorativa, tenuta di un registro su file di log del traffico di rete per avere traccia della navigazione. L'*Istituto* ha il diritto di limitare, o addirittura eliminare, l'accesso dell'utente alla rete per un periodo di tempo, ovvero in modo permanente: in caso di infrazioni alle regole stabilite nelle PUA, che possano danneggiare il corretto funzionamento del sistema a discapito di tutti gli utenti, per queste ragioni il responsabile tecnico delle TIC può effettuare il monitoraggio dei siti visitati dagli utenti della rete, su richiesta del Dirigente Scolastico;
- controllo periodico da parte del responsabile tecnico delle TIC dell'efficacia del sistema di filtraggio;
- settaggio delle macchine in modo tale che agli utenti generici (non amministratori) non siano consentite una serie di operazioni quali installare software; le richieste di installazione di software devono essere rivolte al responsabile tecnico delle TIC;
- utilizzazione e sperimentazione dei software didattici ed educativi open source e/o muniti di regolare licenza. Oltre ai programmi del pacchetto Google Suite for Education, che l'Istituto mette a disposizione nel proprio dominio scolastico, i docenti possono utilizzare, sotto la propria personale responsabilità, altri programmi didattici che abbiano caratteristiche di gratuità, di garanzie sul piano della riservatezza dei dati, della privacy e della sicurezza.
- le comunicazioni ufficiali di natura didattica e amministrativa nella comunità scolastica avvengono tramite registro elettronico, sito istituzionale o mail istituzionale;
- l'utilizzo del laboratorio di informatica è consentito agli studenti solo se accompagnati da un docente responsabile (vedi documento "Regolamento del Laboratorio d'informatica");
- l'utilizzo di chiavi USB, CD o DVD deve essere autorizzato previo controllo antivirus;
- qualora l'*Istituto* riscontri la presenza di materiale illegale o di comportamenti illeciti da parte degli utenti provvederà a riferire alle autorità competenti, secondo le norme di legge.

6 Norme e linee guida

Ferme restando le strategie sistematiche messe in atto dall'*Istituto*, come descritto nel paragrafo precedente, nonché le regole "tacite" di convivenza civile e che disciplinano qualunque rapporto tra le persone (anche su web) e le regole specifiche definite dall'*Istituto* (vedi "Normative e sicurezza" nel sito dell'*Istituto*), tenuto conto del fatto che il sistema di accesso ad internet dell'*Istituto* prevede l'uso di un filtro per evitare l'accesso a servizi o siti web con contenuto non adeguato, ciascun utente deve:

- rispettare la legislazione vigente, applicata anche alla comunicazione su internet, le norme contenute nel presente documento PUA e le indicazioni dirigenziali ricevute in materia di trattamento dei dati e di tutela della privacy (vedi sezione "Normative e sicurezza" nel sito dell'*Istituto*);
- tutelare la propria privacy e quella degli altri componenti della comunità scolastica al fine di non divulgare notizie, dati o informazioni private contenute nelle documentazioni elettroniche a cui ha accesso (vedi "Normativa privacy – vademecum aggiornato);

- rispettare le norme in materia di diritto d'autore;
- rispettare la cosiddetta "netiquette" (regole condivise che disciplinano i rapporti tra utenti della rete e frequentatori di blog, forum, siti, wiki, mail ecc...);
- salvare i propri lavori personali (file) in cartelle personali sull'hard disk o sul web, oppure su dispositivi rimovibili personali (es. chiavette USB) e non sul desktop o nella cartella del programma in uso; i file salvati in modo non corretto potranno essere rimossi a cura del Tecnico responsabile delle TIC;
- non divulgare le credenziali personali di accesso agli account (username e password) di rete, di posta elettronica e/o, nel caso ne sia a conoscenza, alla rete WiFi;
- segnalare prontamente ai responsabili eventuali malfunzionamenti, danneggiamenti, utilizzi impropri o scorretti, violazioni di norme, illeciti;
- non allontanarsi dalla postazione alla quale ha effettuato l'accesso con il proprio account, lasciandola incustodita, se non prima di aver effettuato la corretta disconnessione.

Dopo reiterate violazioni delle regole stabilite dalla politica scolastica, l'*Istituto* ha il diritto di eliminare l'accesso dell'utente a internet per un certo periodo di tempo o in modo permanente.

6.1 Docenti e Personale ATA

I Docenti e tutto il personale sono invitati ad utilizzare quotidianamente e con regolarità nello svolgimento delle proprie attività di servizio, educative e didattiche tutti gli strumenti TIC che ritengono più efficaci ed idonei, nel libero esercizio della propria professionalità, in coerenza con il PTOF dell'*Istituto*. Il personale dell'*Istituto* deve essere sempre consapevole e responsabile del proprio operato nell'utilizzo delle TIC. I Docenti sono inoltre chiamati a vigilare attentamente sugli studenti loro affidati affinché rispettino le regole e le indicazioni normative, nonché mantengano in buono stato ed utilizzino in modo adeguato ed opportuno tutti gli strumenti (hardware e software) a disposizione.
In particolare, ogni insegnante che utilizza le TIC con i propri studenti è chiamato a:

- assolvere in modo professionale e competente il proprio ruolo di educatore, predisponendo anche attività didattiche atte ad indirizzare gli studenti verso una consapevolezza del proprio "agire tecnologico";
- fornire agli studenti chiare indicazioni sul corretto utilizzo di tutte le TIC e sulla rete (internet, posta elettronica, blog, app...), condividendo e discutendo con loro delle regole di buona condotta, dialogando con loro sui rischi della rete (vedi ad esempio sul sito d'*Istituto* "Normative - Linee di orientamento contro il cyberbullismo"), vigilando sul rispetto delle regole e promuovendo negli studenti una "educazione digitale", informandoli del monitoraggio della navigazione e delle sanzioni in caso di violazioni consapevoli delle norme;
- prestare attenzione al rischio di accesso da parte di terzi a dati personali e/o sensibili, non salvando mai sulla memoria locale di postazioni comuni file contenenti dati personali e/o sensibili, e-mail, documenti, ecc... (vedi ad esempio sul sito d'*Istituto* "Normativa privacy – vademecum aggiornato");
- vigilare che durante le lezioni l'accesso degli studenti alla rete internet avvenga sotto la propria supervisione e unicamente con gli strumenti autorizzati e/o messi a disposizione dall'Istituto;
- richiedere tempestivamente al responsabile tecnico delle TIC di controllare, quando ritenuto opportuno e/o all'evenienza in caso di episodi sospetti o dubbi, le azioni compiute dagli studenti (ad esempio analizzando tempestivamente la cronologia, i files temporanei, i cookies, ecc...);

L'Istituto mette a disposizione dei docenti spazi virtuali (registro elettronico ARGO, servizi di GSuite for Education) il cui utilizzo agevola tutti gli utenti dal punto di vista tecnico e li tutela nei rapporti istituzionali. Nel rispetto della libertà di insegnamento, ogni docente può utilizzare altri strumenti, sempre però sotto la propria personale responsabilità.
L'*Istituto* si impegna ad attivare azioni formative nei confronti di tutto il personale, come richiesto dal Regolamento Europeo UE 2016/679.
È inoltre fondamentale che i docenti educhino gli studenti al rispetto della normativa sui diritti d'autore (per approfondimenti si rimanda al sito: http://www.garanteprivacy.it)

Estratto dalla legislazione vigente sui Diritti d'Autore (Legge del 22 aprile 1941 n° 633 art. 70)
"... il riassunto, la citazione o la riproduzione di brani o di parti di opera per scopi di critica di discussione ed anche di insegnamento, sono liberi nei limiti giustificati da tali finalità e purché non costituiscano concorrenza all'utilizzazione economica dell'opera".

Quindi, se nel realizzare lavori didattici o pagine web, l'autore inserisce a scopo di discussione, di critica, di informazione culturale, parti di opere, brevi estratti o citazioni (mai l'opera integrale) citando chiaramente e correttamente il nome dell'autore e la fonte, non incorre in problemi di copyright. In questi casi, infatti, l'autore delle opere non sarà danneggiato nei suoi diritti anzi potrebbe acquistare maggiore notorietà.

6.2 Studenti

Gli studenti sono chiamati ad utilizzare tutte le TIC a loro disposizione a fini educativi e didattici, coerentemente con le indicazioni dei propri docenti. Ogni comportamento che sia volto a perseguire finalità diverse da quelle pedagogiche, educative e didattiche, non è consentito.
Gli studenti sono tenuti a rispettare i regolamenti contenuti nella sezione "Normative e sicurezza" del sito d'Istituto, nell'utilizzo degli spazi fisici e virtuali messi a disposizione dell'*Istituto*.
In particolare, gli studenti sono tenuti a:

- utilizzare le TIC loro fornite dai docenti e/o dall'*Istituto* per lo svolgimento delle attività autorizzate, sotto la supervisione del docente. È possibile anche l'utilizzo all'interno dell'*Istituto* di strumenti tecnologici personali (modalità BYOD) ma sempre sotto la supervisione del docente ed unicamente per scopi didattici;
- utilizzare chiavette USB, CD, CD-ROM, DVD, memory card o altri dispositivi esterni personali previa autorizzazione di un docente responsabile;
- accedere sempre alla rete con le proprie credenziali personali ovvero nelle modalità indicate dal docente responsabile;
- archiviare i propri documenti secondo le modalità indicate dai docenti e chiudere sempre correttamente la propria sessione di lavoro al termine del suo utilizzo;
- non eseguire tentativi non espressamente autorizzati di modifica della configurazione del sistema dei dispositivi informatici;
- non utilizzare giochi né in locale né in rete, a meno che non abbiano una valenza didattica e siano stati suggeriti da un docente;
- comunicare tempestivamente ai responsabili il riscontro di eventuali malfunzionamenti della strumentazione e/o di comportamenti scorretti, pericolosi o inappropriati da parte propria o di altri;
- mantenere segrete e custodire con cura le proprie credenziali (username e password) di accesso agli spazi virtuali dell'*Istituto*;
- oltre alle password è bene non comunicare mai a terzi (soprattutto in rete) i propri dati personali quali i dati anagrafici, indirizzo, telefono, ecc...

- non mettere in rete fotografie o video personali o di amici e comunque ogni genere di materiale non appropriato;
- riferire immediatamente ai docenti responsabili qualora qualcuno tenti un contatto dall'esterno tramite la rete e/o invii materiale inopportuno di ogni genere;
- ricordare sempre che in rete è difficile verificare l'identità delle persone e che pertanto si possono incontrare estranei che forniscono identità e informazioni false e non attendibili;
- discutere sempre e confrontarsi apertamente con i propri docenti in caso di dubbi o di incertezze sui comportamenti più appropriati da adottare in relazione alle TIC dell'*Istituto*;
- non utilizzare strumenti digitali personali (smartphone, tablet…etc) durante le lezioni per uso personale, è possibile invece utilizzarli in modalità BYOD, per finalità didattiche e con l'autorizzazione del docente.

Per gli studenti maggiorenni è richiesta una autorizzazione alla pubblicazione di immagini (foto e video), della voce o di prodotti (es. lavori, disegni, ecc...) da loro realizzati, da utilizzare esclusivamente per scopo documentario, didattico e scientifico, secondo le finalità proprie della scuola, in qualunque forma o modo, in Italia o all'estero, senza limitazione di spazio e tempo e senza compensi di sorta. Per le autorizzazioni relative agli studenti minorenni si veda la sezione 6.3 Genitori/Tutori.

6.3 Genitori/Tutori

Le famiglie degli studenti sono invitate a collaborare con la scuola per una sana ed efficace educazione dei ragazzi ad un utilizzo corretto e sicuro delle TIC, in un rapporto di costruttivo "dialogo educativo".

Ai genitori (o esercenti la patria potestà) viene richiesto:

- di prestare attenzione ai principi e alle regole per un corretto utilizzo delle TIC, sintetizzate in questo documento, nonché di segnalare prontamente a Docenti e Coordinatori Didattici il sospetto, ovvero la fondata conoscenza di comportamenti pericolosi o inappropriati da parte dei propri figli relativamente alle TIC dell'Istituto;
- di presentare una autorizzazione alla pubblicazione di immagini (foto e video), della voce o di prodotti (es. lavori, disegni, ecc...) dei propri figli (minori e non), da utilizzare esclusivamente per scopo documentario, didattico e scientifico, secondo le finalità proprie della scuola, in qualunque forma o modo, in Italia o all'estero, senza limitazione di spazio e tempo e senza compensi di sorta;
- di presentare una autorizzazione per l'utilizzo a scuola di un account personale dell'alunno sotto il dominio liceoeqvisconti.it, appoggiato su piattaforma G Suite for Education, (si veda sul sito dell'*Istituto*, nella sezione "Normative e sicurezza", il "Regolamento d'uso di G Suite for Education"). Tali strumenti sono forniti dall'*Istituto* nel rispetto delle norme di legge e sono da impiegarsi per lo svolgimento delle attività didattiche e formative in rete. È diritto dei genitori rifiutare tale autorizzazione, consapevoli che, in caso di rifiuto, sono tenuti a fornire un indirizzo di posta elettronica alternativo sotto la loro responsabilità compatibile con le richieste e le esigenze didattiche e tecniche, al fine di non escludere il proprio figlio dalle attività svolte con le TIC.

Allo scopo di condividere regole comuni per l'utilizzo sicuro di internet, sia a casa che a scuola si invitano i genitori/tutori a prestare la massima attenzione ai principi e alle regole per un utilizzo consapevole delle TIC, sintetizzate in questo documento, impegnandosi a farle rispettare ai propri figli, possibilmente anche in ambito domestico, primariamente assistendo sempre i minori nel momento dell'utilizzo della rete e delle TIC, nonché dialogando con loro e ponendo in atto tutti i sistemi di sicurezza che aiutino a minimizzare il rischio di incorrere in materiale pericoloso o comunque indesiderato.

7 Informare sulla Politica d'Uso Accettabile (PUA) dell'Istituto

Questo documento e gli altri documenti correlati sono sempre visionabili sul sito dell'*Istituto* e saranno diffusi agli utenti delle TIC tramite circolare alla prima emissione o alle successive modifiche.
Gli utenti delle TIC all'atto della consegna delle credenziali di accesso alle risorse d'*Istituto* o della prima emissione delle PUA, dovranno dichiarare di aver preso visione del presente documento e dei documenti ad esso correlati.

7.1 Informare gli studenti sulla PUA dell'Istituto

Le regole di base relative all'accesso ad internet saranno sempre disponibili attraverso il sito dell'*Istituto*. Prendendo visione delle PUA gli studenti saranno informati che l'utilizzo di internet è monitorato ed avranno così le indicazioni per un uso responsabile e sicuro di internet. Nel Patto di Corresponsabilità studenti e genitori si impegnano a rispettare quanto previsto nel PUA e nei Regolamenti.

7.2 Informare il personale scolastico della PUA

Tutto il personale scolastico, docente e ATA, si deve considerare coinvolto nello sviluppo delle linee guida delle PUA d'*Istituto*. Il personale è tenuto a prendere visione delle PUA, a rispettarne le regole e ad assumersi la responsabilità del proprio operato relativamente all'uso delle TIC, consapevole che ogni eventuale abuso verrà segnalato alle Autorità competenti.
In caso di dubbi legati alla legittimità di una certa risorsa utilizzata in internet, il docente dovrà contattare il Dirigente Scolastico e i componenti del Gruppo PNSD, per evitare malintesi. I docenti, nella sezione normativa del sito web dell'*Istituto*, trovano le informazioni concernenti le problematiche sui diritti d'autore applicate alla scuola.

7.3 Informare i genitori/tutori sulla PUA della scuola

I genitori sono informati della PUA dell'*Istituto* tramite circolari e comunicazioni sul sito dell'*Istituto*.
L'*Istituto* deve chiedere ai genitori/tutori degli studenti minori il consenso all'uso di internet per il loro figlio ed alla pubblicazione dei suoi lavori e delle sue immagini. Nel caso di studenti maggiorenni il consenso alla pubblicazione dei lavori e delle immagini deve essere dato anche dagli studenti stessi.