



Istituto di Istruzione Superiore “Arturo Prever”

Integrazione al Regolamento di Istituto e al PTOF in merito alla Sicurezza Informatica
ed Uso Consapevole delle TIC Nella scuola

REGOLE PER L'USO CORRETTO E CONSAPEVOLE DELLA RETE a.s. 2016/17

Il seguente regolamento è redatto al fine di garantire le norme previste dalle leggi di riferimento:

- L. 633/1941, Testo consolidato al 9 febbraio 2008, Protezione del diritto d'autore e di altri diritti connessi al suo esercizio;
- D. lgs 305/2006 del 07/12/2006, Regolamento recante identificazione dei dati sensibili e giudiziari trattati e delle relative operazioni effettuate dal Ministero della pubblica istruzione, in attuazione degli articoli 20 e 21 del Dlgs 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali;
- L. 4/2004, Disposizioni per favorire l'accesso dei soggetti disabili agli strumenti informatici;
- D. lgs 196/2003 Testo Unico sulla privacy entrato in vigore il 01/01/2004 che riassume le norme precedenti sulla privacy;
- D. lgs 68/2003, Sulla regolamentazione per la tutela del diritto d'autore e dei diritti connessi nella società dell'informazione;
- C. M. 114/2002, Sulle infrastrutture tecnologiche nelle scuole e nuove modalità di accesso al sistema informativo.
- C.M. 152/2001, Sulla diffusione delle reti LAN;
- L. 325/2000, Sull'adozione delle misure di sicurezza nel trattamento dei dati in applicazione dell'art.15 della Legge 675/1996;
- L. 248/2000, Nuove norme di tutela del diritto d'autore;
- D.P.R. n. 275 del 25/02/1999, Regolamento recante norme in materia di autonomia delle istituzioni scolastiche, ai sensi dell'art. 21 della legge 15 marzo 1997, n. 5;
- L. 547/1993, Norme in materia di reati informatici;

SCOPO DI UNA POLITICA D'USO accettabile e sicuro della rete della scuola

Scopo del presente documento è quello di informare l'utenza al fine di garantire un uso corretto e responsabile delle apparecchiature informatiche collegate alla rete in dotazione alla Scuola, nel rispetto della normativa vigente.

Il modello didattico "sperimentale" introdotto da Community Prever, previsto dal PNSD (Piano Nazionale Scuola Digitale), come introduzione di metodologie didattiche innovative, e l'uso delle LIM, prevede l'utilizzo delle Tecnologie dell'Informazione e della Comunicazione (di seguito TIC) da parte degli insegnanti e degli alunni.

Gli utenti, siano essi maggiorenni o minori, devono essere pienamente consapevoli dei rischi a cui si espongono quando navigano in rete. Di fatto esiste la possibilità che durante il lavoro online si possa entrare accidentalmente in contatto con materiale inadeguato e/o illegale, pertanto la Scuola promuove l'adozione di strategie che limitino l'accesso a siti e/o applicazioni illeciti: è infatti dovere della Scuola garantire il diritto all'accesso alla rete e adottare nel contempo tutti i sistemi di sicurezza conosciuti per diminuire le possibilità di rischio nella navigazione.

In questo contesto, gli insegnanti hanno la responsabilità di guidare gli studenti nelle attività online a scuola e di stabilire regole di condotta chiare per un uso critico e consapevole di Internet anche a casa, per prevenire il verificarsi di situazioni potenzialmente pericolose.

Resta fermo che non è possibile garantire una navigazione totalmente priva di rischi e che la Scuola e gli insegnanti non possono assumersi le responsabilità conseguenti all'accesso accidentale e/o improprio a siti illeciti, ed al reperimento ed uso di materiali inappropriati.

Prima di firmare il documento, tutte le parti in causa devono leggerle attentamente per accertarsi di averle comprese in tutte le parti e di accettarne i contenuti.

I vantaggi di Internet a scuola

Il percorso formativo scolastico prevede il regolare utilizzo dei laboratori informatici dove, oltre a svolgere le normali attività tecniche inerenti la specializzazione, gli studenti imparano a trovare materiale, recuperare documenti e scambiare informazioni utilizzando le TIC. Inoltre da quest'anno l'Istituto si è dotato di un'infrastruttura di rete wireless che fornisce la connettività a insegnanti e studenti delle diverse sedi.

Internet offre sia agli studenti che agli insegnanti una vasta scelta di risorse diverse e opportunità di scambi culturali con gli studenti di altri paesi. Inoltre su internet si possono recuperare risorse per il tempo libero, le attività scolastiche e sociali.

La scuola propone agli studenti e agli insegnanti di utilizzare Internet non soltanto per le attività didattiche e sociali ma anche per promuovere l'eccellenza in ambito didattico attraverso la condivisione delle risorse, l'innovazione e la comunicazione. Per gli studenti e per gli insegnanti l'accesso ad internet, nel rispetto delle disposizioni del Ministero dell'Istruzione Università e Ricerca che vietano l'uso in classe di telefoni cellulari e dispositivi elettronici, è un privilegio e un diritto. Poiché esiste la possibilità che gli studenti trovino materiale inadeguato e illegale su internet, la scuola ha limitato l'accesso ad internet mediante firewall e le attività svolte in rete vengono monitorate e tracciate nel rispetto delle vigenti normative sulla privacy. Il firewall da solo non è però in grado di eliminare tutti i rischi e gli studenti sono in grado collegarsi ad Internet senza protezione sia da casa che con il proprio cellulare.

Inoltre il regolamento non va riferito solo ai pericoli presenti in Internet, ma anche alla rete interna dell'Istituto, il cui uso improprio può generare problemi da un punto di vista didattico, difficoltà di uso delle macchine, fino al blocco delle stesse, comportando un danno funzionale ed anche economico.

Per questi motivi gli insegnanti hanno la responsabilità di guidare gli studenti nelle attività online, di stabilire obiettivi chiari nell'uso di Internet, insegnando un uso dei nuovi strumenti

di comunicazione accettabile e responsabile. L'obiettivo principale resta quello di arricchire ed ampliare le attività didattiche, secondo quanto prevede il curriculum scolastico, l'età e la maturità degli studenti.

Le presenti Regole che forniscono le linee guida per il benessere e la sicurezza di tutti gli utenti della rete, sono pubblicate sul sito dell'istituto, esposte nei laboratori e vengono consegnate a studenti e docenti che richiedono l'accesso alla rete wireless.

Strategie attuate dalla scuola per garantire la sicurezza delle TIC

La scuola si fa carico di tutte le precauzioni necessarie per garantire agli studenti l'accesso a materiale appropriato, ma gli studenti devono essere pienamente coscienti dei rischi a cui si espongono quando sono in rete. Devono essere educati a riconoscere e a evitare gli aspetti negativi di internet come la pornografia, la violenza, il razzismo e lo sfruttamento dei minori.

- Il sistema di accesso a internet della scuola prevede l'uso di un firewall per la navigazione per evitare l'accesso a chat non moderate, gruppi di discussione o siti web con contenuto non appropriato.
- Il sistema informatico delle TIC della scuola viene regolarmente controllato dallo staff tecnico in base alle norme di sicurezza.
- È vietato inserire file sul server o scaricare da internet software non autorizzati o materiale soggetto a diritti di autore (file musicali, video, ecc.). L'insegnante controlla che venga rispettato questo divieto dagli allievi.
- Il sistema informatico della scuola è provvisto di un software antivirus aggiornato periodicamente dallo staff tecnico.
- Per utilizzare pen drive CD-ROM e DVD o altri supporti di memorizzazione personali è necessario chiedere un permesso e sottoporli al controllo antivirus
- In generale il software utilizzabile è solamente quello autorizzato dalla scuola, regolarmente licenziato e/o open source (o freeware).

Norme e linee guida

Fra gli utenti dei servizi telematici Internet si sono sviluppati nel corso del tempo una serie di principi di buon comportamento che vengono identificati con il nome di Netiquette. Con l'avvento del web 2.0 e dei Social Network, basati sui principi di collaborazione e condivisione diretta degli utenti, internet e i suoi servizi si sono evoluti, dando vita ad un galateo del web 2.0 che prende il nome di Netiquette 2.0

Questi principi sono le linee guida fondamentali per la sicurezza e il benessere di tutti nella rete, in particolare negli ambienti più usati dagli adolescenti.

Tutti gli utenti della rete dell'Istituto devono rispettare scrupolosamente questi principi, le leggi vigenti in materia di diritto d'autore e tutela della privacy nonché le specifiche norme penali relative al settore informatico e della comunicazione elettronica, oltre ad ogni altra disposizione generale di legge.

Reati e violazioni della legge

Al di là delle regole di buona educazione ci sono comportamenti, talvolta solo apparentemente innocui, che possono portare gli autori a commettere veri e propri reati e, di conseguenza, a subire procedimenti penali dalle conseguenze molto serie.

Reati informatici: la legge 547/93 individua e vieta tutta una serie di comportamenti nell'ambito informatico e che sono stati reputati lesivi per gli interessi non solo di singoli privati cittadini ma anche di persone giuridiche, in particolare per le imprese e gli enti pubblici.

Accesso abusivo ad un sistema informatico e telematico o Attività di introduzione in un sistema, a prescindere dal superamento di chiavi "fisiche" o logiche poste a protezione di quest'ultimo. Art. 615 ter cp. o Per commettere il reato basta il superamento della barriera di protezione del sistema o accedere e controllare via rete un PC a insaputa del legittimo proprietario, oppure forzare la password di un altro utente e più in generale accedere abusivamente alla posta elettronica, ad un server o ad un sito su cui non siamo autorizzati.

Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico o L'art 615 quinquies punisce "chiunque diffonde, comunica o consegna un programma informatico da lui stesso o da altri creato, avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento".

Per commettere questo reato basta, anche solo per scherzo, diffondere un virus, spiegare ad altre persone come si può fare per rendere accessibile un computer, un software o una console per giochi oppure anche solo controllare a distanza o spegnere un computer via rete.

Danneggiamento informatico

Per danneggiamento informatico si intende un comportamento diretto a cancellare o distruggere o deteriorare sistemi, programmi o dati. L'oggetto del reato, in questo caso, sono i sistemi informatici o telematici, i programmi, i dati o le informazioni altrui. Art. 635 cp.

Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici

Questo particolare reato viene disciplinato dall'art. 615 quater cp e si presenta spesso come complementare rispetto al delitto di frode informatica. Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici È considerato reato anche quando l'informazione viene fraudolentemente carpita con "inganni" verbali e quando si prende conoscenza diretta di documenti cartacei ove tali dati sono stati riportati o osservando e memorizzando la "digitazione" di tali codici. Si commette questo reato quando si carpiscono, anche solo per scherzo, i codici di accesso alla posta elettronica, o al profilo di amici e compagni.

Frode informatica

Questo delitto discende da quello di truffa e viene identificato come soggetto del reato "chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità sui dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno". Art. 640 ter cp.

Il profitto può anche "non avere carattere economico, potendo consistere anche nel soddisfacimento di qualsiasi interesse, sia pure soltanto psicologico o morale". Il delitto di frode informatica molto sovente viene a manifestarsi unitamente ad altri delitti informatici, quali l'Accesso informatico abusivo e danneggiamento informatico in conseguenza a Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico. Reati non informatici: sono da considerare reati non informatici tutti quei reati o violazioni del codice

civile o penale in cui il ricorso alla tecnologia informatica non sia stato un fattore determinante per il compimento dell'atto.

Ingiuria

Chiunque offende l'onore o il decoro di una persona presente commette il reato di ingiuria. Incorre nello stesso reato chi commette il fatto mediante comunicazione telegrafica o telefonica o con scritti, o disegni, diretti alla persona offesa.

Diffamazione

Qualcuno che offende la reputazione di qualcun altro, quando all'interno di una comunicazione con più persone si diffondono notizie o commenti volti a denigrare una persona. Art. 595 cp.

Aggravante nel caso in cui l'offesa sia recata con un "mezzo di pubblicità" come l'inserimento, ad esempio, in un sito Web o social network di una informazione o un giudizio o un soggetto. La pubblicazione online, dà origine ad un elevatissimo numero di "contatti" di utenti della Rete, generando un'incontrollabile e inarrestabile diffusione della notizia.

Minacce e molestie

Il reato di minaccia consiste nell'indirizzare ad una persona scritti o disegni a contenuto intimidatorio per via telematica. Art. 612 cp.

Può capitare che alcune minacce vengano diffuse per via telematica anche per finalità illecite ben più gravi: come ad esempio obbligare qualcuno a "fare, tollerare o omettere qualche cosa" (Violenza privata: art. 610 cp.) o per ottenere un ingiusto profitto (Estorsione: art. 629 cp.).

Sull'onda di questa tipologia di reati, è utile descrivere anche quello di Molestie e disturbo alle persone, disciplinato dall'art. 660 cp. che si fonda sul contattare, da parte di terzi, per finalità pretestuose, il soggetto i cui dati sono stati "diffusi" per via telematica.

Ad esempio la pubblicazione del nominativo e del cellulare di una persona online, accompagnato da informazioni non veritiere o ingiuriose: ciò potrebbe indurre altre persone a contattare la persona per le ragioni legate alle informazioni su questa fornite.

Violazione dei diritti d'autore

La legge 159/93 sottolinea all'art. 1 che chiunque abusivamente riproduce a fini di lucro, con qualsiasi procedimento, la composizione grafica di opere o parti di opere letterarie, drammatiche, scientifiche, didattiche e musicali, che siano protette dalla legge 22 aprile 1941, n. 633 e successive modificazioni, ovvero, pone in commercio, detiene per la vendita o introduce a fini di lucro le copie viola i diritti d'autore.

Un primo caso di violazione del diritto d'autore si può verificare quando una copia non autorizzata di un'opera digitale è caricata su un server e messa a disposizione degli utenti.

In questo caso, colui che riproduce e fornisce l'opera senza l'autorizzazione da parte del suo autore è considerato soggetto responsabile. Per commettere questo reato basta pubblicare su YouTube un video con una qualsiasi musica di sottofondo senza le dovute autorizzazioni.

Un ulteriore possibile violazione del diritto d'autore si verifica quando l'utente ottiene il documento, il software o il brano mp3 messo a disposizione in rete o acquistato e ne fa un uso illegittimo, come ad esempio, rivenderlo a terzi o distribuirlo sulla Rete facendone più copie non autorizzate.

La legge italiana sul diritto d'autore consente all'utilizzatore di un software o di un'opera multimediale o musicale di effettuare un'unica copia di sicurezza ad uso personale, utile nei casi di malfunzionamento del programma, smarrimento della copia originale etc. Tale copia, salvo autorizzazione della casa di produzione, non può essere ceduta ad altre persone.

La duplicazione abusiva (senza autorizzazione) è sanzionata penalmente e colpisce ugualmente anche chi duplica abusivamente non a scopo di lucro, bensì per un semplice fine di risparmio personale.

Informare sulle Regole per l'uso corretto e consapevole della rete della scuola: studenti – personale – genitori

Le regole di base relative all'accesso ad internet verranno esposte nei laboratori di informatica e pubblicate sul sito. Gli studenti saranno informati che l'utilizzo di internet è monitorato e verranno date delle istruzioni per un uso responsabile e sicuro di internet.

Il personale scolastico avrà una copia del documento e dovrà sottoscriverlo, ed è consapevole che l'uso di internet verrà monitorato e controllato. In caso di dubbi legati alla legittimità di un servizio utilizzato in internet, l'insegnante dovrà contattare il D.S. per evitare malintesi. Gli insegnanti saranno provvisti di informazioni concernenti le problematiche sui diritti d'autore che vengono applicate alla scuola.

I genitori degli studenti minorenni che a scuola non vogliono far usare internet ai loro figli e non desiderano che i loro lavori e le loro fotografie siano pubblicati, devono far pervenire in istituto presso la segreteria una dichiarazione di esonero.

La posta elettronica

Gli studenti durante le attività didattiche non possono utilizzare il servizio e-mail personale se questo interferisce con altre attività di apprendimento. In altri momenti scolastici possono accedere al servizio e-mail personale previa richiesta ai docenti. Gli studenti devono utilizzare durante l'orario scolastico solo fornitori di servizi e-mail approvati dall'Istituto. Gli studenti devono riferire agli insegnanti se ricevono e-mail offensive.

Gli studenti non devono rivelare dettagli o informazioni personali proprie o di altre persone di loro conoscenza, come indirizzi, numeri di telefono, o organizzare via web o mail, incontri fuori dalla scuola. L'invio e la ricezione di allegati è soggetto al permesso dell'insegnante. Per tutti gli utilizzatori di internet è consentita la consultazione della propria e-mail personale solo attraverso un dominio istituzionale. Non è garantita la consultazione della propria e-mail attraverso un dominio privato poiché potrebbero contenere materiali e/o servizi non conformi al presente regolamento.

Gli utenti che leggono i propri messaggi sul server dei servizi di posta non devono lasciarne traccia sui computer dell'istituto; non è consentito configurare un client di posta locale per la lettura di e-mail né al personale né agli allievi; solo in casi particolari e in presenza di una ben precisa programmazione di disciplina, i responsabili delle TIC potranno configurare un client di posta locale per la lettura di e-mail al fine di favorire scambi culturali.

Un indirizzo e-mail può essere attribuito a un gruppo di studenti o a una classe nel caso di attività didattiche che prevedano scambio d'informazioni con altri.

Gestione del sito web della scuola

La redazione editoriale dell'Istituto, costituita dal Dirigente Scolastico, dal Responsabile Sito Web, dal DSGA, gestisce le pagine del sito, ed eventuali altre forme di presenza in rete sui diversi social network (Facebook, Instagram, Tweeter ecc.) , approvati dal Collegio dei Docenti e dal Consiglio di Istituto, ed è sua responsabilità garantire che il contenuto sul sito o su altri social network, sia accurato e appropriato.

Per evitare confusione negli utenti, le informazioni istituzionali relative alle attività didattiche, orari, circolari, concorsi, manifestazioni ecc, devono essere pubblicate esclusivamente sul sito di istituto e non sono consentite altre forme di pubblicazione su altri mezzi di comunicazione.

Il sito di istituto assolverà alle linee guida sulle pubblicazioni dell'Istituto, come definito nel [Programma Triennale per la trasparenza e l'Integrità](#)

L'Istituto detiene i diritti d'autore dei documenti che si trovano sul sito, oppure è legittimato a utilizzarli avendo chiesto e ottenuto il permesso all'autore che ne è proprietario. Le informazioni pubblicate sul sito dell'Istituto relative alle persone devono includere solo l'indirizzo di posta elettronica e il telefono dell'Istituto, ma non informazioni relative agli indirizzi del personale della scuola o altre informazioni del genere.

L'istituto offre, all'interno del proprio sito web, tutta una serie di servizi alle famiglie e agli utenti esterni:

- orari delle classi, dei docenti, delle strutture;
- informazioni sulle iniziative e sui progetti;
- comunicazioni alle famiglie;
- reperimento di modulistica;
- accesso ad ipertesti didattici pubblicati su www.spazioprever.it;
- accesso alla Community Prever e ai blog di pubblicazione
- altre informazioni;
- tramite l'accesso al sito del registro elettronico, valutazioni degli allievi (accesso riservato all'utenza tramite nome utente e password personali).

Tali servizi sono erogati in conformità con quanto espresso della Legge 196/2003 in materia del trattamento dei dati e della legge 9 gennaio 2004, n.4 "Disposizioni per favorire l'accesso dei soggetti disabili agli strumenti informatici" e la legge n. 69 del 18 giugno 2009 sulla trasparenza dei siti della Pubblica Amministrazione.

Si precisa che tutti i servizi offerti non trattano dati sensibili, ovvero dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

Mailing list moderate, gruppi di discussione e chat room

- L'Istituto può utilizzare una lista d'indirizzi di utenti selezionati per distribuire del materiale.
- L'insegnante è il moderatore degli altri mezzi di collaborazione, dei gruppi di discussione e delle chat room se sono utilizzati in Istituto.
- Agli studenti non è consentito l'accesso alle chat room pubbliche o non moderate.
- Sono permesse solo chat a scopi didattici e comunque sempre con la supervisione dell'insegnante per garantire la sicurezza.
- Solo i gruppi di discussione che hanno obiettivi e contenuti didattici sono disponibili agli studenti.

Linee guida per alunni e docenti

Le informazioni che seguono sono delle linee guida per l'utilizzo delle TIC e per la navigazione in Rete. Alcuni di questi consigli riguardano l'uso sicuro della Rete anche a casa.

Agli alunni si consiglia di:

- Mantenere segreto il nome, l'indirizzo, il telefono di casa, il nome e l'indirizzo della scuola che frequentate.
- Disconnettersi sempre (log out) dai siti che hanno richiesto password e nome utente per l'accesso (log in) .
- Non inviare a nessuno fotografie proprie o di loro amici.
- Registrarsi con nome ed e-mail solo su siti individuabili senza il minimo dubbio
- Chiedere sempre all'insegnante o a un adulto il permesso di scaricare documenti dalla Rete.
- Chiedere sempre il permesso prima di iscriversi a qualche concorso o prima di riferire l'indirizzo della scuola.
- Riferire all'insegnante se qualcuno invia loro immagini che li infastidiscono e non rispondere mai a queste mail. Riferire anche all'insegnante se capita di trovare immagini di questo tipo in Rete.
- In caso di accesso fortuito a siti illegali (es. pedofilia) sfuggiti al filtro Internet, disconnettersi immediatamente e avvertire l'insegnante fornendo l'URL del sito oppure quello della pagina Web che ha condotto al sito, in modo che esso possa essere immediatamente inserito nella black list. È necessario spiegare chiaramente agli utenti che questi siti sono monitorati dalla Polizia Postale e che un accesso reiterato può significare l'iscrizione a una lista di persone da indagare.
- Scegliere password di accesso alla rete non banali e non comunicarle ad altri per nessun motivo. Il nome utente e la relativa password costituiscono il metodo con cui viene identificata la persona che ha fatto l'accesso alla rete.
- Se qualcuno in Rete chiede un incontro di persona, riferirlo o all'insegnante o a un adulto e non rispondere in nessun caso all'invito. Occorre ricordare che le persone che s'incontrano nella Rete sono degli estranei e non sempre sono quello che dicono di essere.

- Non è consigliabile inviare messaggi di posta elettronica personali, perciò chiedere sempre al proprio insegnante prima di inviare messaggi di classe.
- Non caricare o copiare materiale dalla Rete senza il permesso dell'insegnante e del responsabile dei laboratori.
- In caso di allontanamento dalla propria postazione di lavoro, bloccare la workstation in modo tale che un altro utente non possa commettere abusi con le nostre credenziali.

Ai docenti si consiglia:

- Ogni insegnante è garante nei confronti del dirigente scolastico dell'utilizzo della piattaforma in base alle disposizioni presenti in questo documento e più in generale al codice disciplinare e al codice di condotta.
- Evitare di lasciare posta e documenti sull' hard disk delle macchine della scuola lo spazio è limitato.
- Ottimizzare le dimensioni delle immagini pubblicate in rete, si risparmia la banda degli utenti e le pagine si caricano più velocemente.
- I documenti di scuola vanno conservati su dispositivi di memorizzazione (pen drive, cd, dvd) di proprietà degli insegnanti. Per quanto riguarda il trattamento e l'archiviazione di dati personali degli alunni si rimanda alle indicazioni contenute nella lettera di nomina a incaricato al trattamento dei dati che ogni docente ha ricevuto.
- Al termine dell'anno scolastico i documenti memorizzati sui computer saranno cancellati dal Responsabile dei laboratori.
- Disconnettersi sempre (log out) dai siti che hanno richiesto password e nome utente per l'accesso (log in) .
- Discutere con gli alunni della PUA della scuola e degli eventuali problemi che possono verificarsi nell'applicazione delle regole relative all'uso della Rete.
- Registrare sempre l'accesso al laboratorio
- Dare chiare indicazioni su come si utilizza la Rete e la posta elettronica, e informate gli alunni che le navigazioni saranno monitorate.
- Ricordare agli alunni di chiudere la connessione (e di spegnere le macchine) alla fine della sessione di lavoro sulla Rete. Controllate alla fine che tutti i computer siano spenti.
- Ricordare agli alunni che la violazione consapevole della PUA della scuola comporta la temporanea o permanente sospensione dell'accesso alla Rete.
- Riferire al Fornitore del Servizio di connessione alla Rete o alla polizia di eventuali siti pedopornografici.
- L'insegnante deve controllare che le fonti siano sempre citate dagli alunni. Di norma occorre il permesso per riprodurre materiali quali testi, suoni, immagini o video clips. Per questo è importante controllare sempre le leggi sul copyright. In molti casi questo è possibile e molti autori darebbero volentieri il permesso. Basta chiedere e citare la fonte. Se ciò non è possibile occorre comunque citare sempre la fonte dei materiali che si utilizzano (testi, immagini, video clips e suoni).

Eventuali commenti o suggerimenti connessi alla Politica d'Uso Accettabile delle Reti e delle TIC possono essere inviati al seguente indirizzo: iisprever.gov.it@iisprever.gov.it

N.B. La violazione delle regole stabilite dalla politica scolastica dà alla Scuola il diritto di bloccare l'accesso dell'utente ad internet per un certo periodo di tempo o in modo permanente.

Allegato

Principi di comportamento consapevole in rete

Internet favorisce la libertà d'espressione e, quando si entra a far parte di una community o di un servizio dove interagiscono più utenti, devono essere considerati abusi da segnalare 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, Netlog, ecc..., 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, scegliendo con cura le amicizie con cui accrescere la propria rete e i gruppi a cui aderire e proteggendo la propria identità digitale con password complesse e usando una domanda di recupero password dalla risposta non scontata.

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.

Relazioni tra persone di pari livello – (Rapporto 1 a 1)

All'interno dei Social Network si instaurano tante relazioni tra singoli utenti, non veicolate o controllate da intermediari, chiamati rapporti di pari livello. È importante fare attenzione a quali informazioni vengono fornite in questo contesto, evitando di condividere dati personali e di contatto, come numeri di telefono o indirizzi, che nella vita reale non si darebbero a persone che non sono ancora degne di fiducia.

Bisogna evitare di scambiare file con utenti di cui non ci si può fidare e in ogni caso, anche quando si conosce l'interlocutore, è necessario verificare sempre l'origine dei file ed effettuarne un controllo con un antivirus aggiornato.

Se durante una chat, un forum o in una qualsiasi discussione online, l'interlocutore diviene volgare, offensivo o minaccioso, si deve evitare di fomentarlo, ignorandolo e abbandonando la conversazione.

Quando si riscontra un comportamento riconducibile ad un illecito durante una conversazione privata, per esempio un tentativo di approccio sessuale nonostante la minore età, stalking o cyberbullismo, l'utente può sfruttare gli appositi sistemi di reportistica degli abusi predisposti all'interno del servizio, segnalando tempestivamente il nickname che ha perpetrato l'abuso. In questi casi può essere conveniente abbandonare non soltanto la conversazione ma anche il profilo personale usato fino a quel momento creandosene uno nuovo.

Quando si fa uso di sistemi di [file-sharing P2P](#), è importante evitare di scaricare dei file che possono essere considerati illegali e protetti dal diritto d'autore. Bisogna inoltre fare attenzione e non aprire mai dei file sospetti, verificandone la bontà con un antivirus aggiornato; La maggior parte dei programmi P2P contiene spyware e malware, software malevoli in grado di compromettere seriamente la sicurezza del computer che si sta usando. Per motivi di sicurezza della rete l'utilizzo questi sistemi a scuola è vietato.

I sistemi di messaggistica dei Social Network hanno le stesse regole della posta elettronica quindi è necessario preservare la privacy di tutti, cancellando il mittente o i vari destinatari quando si invia

un messaggio a più destinatari che non si conoscono tra loro, evitare di inoltrare spam o catene di sant'Antonio, o perpetrare qualunque tipo di abuso usando i messaggi elettronici.

Contenuti generati dagli utenti – (Rapporto 1 a N)

I contenuti pubblicati sulle applicazioni web dei Social Network, hanno diversi livelli di visibilità, per esempio singoli utenti o tutti gli utenti della rete, che devono sempre essere tenuti a mente, dando a ciascun contributo i corretti livelli di privacy. Pertanto, quando si inizia a pubblicare materiale in una community bisogna studiare ed imparare ad utilizzare correttamente le funzioni per l'impostazione dei livelli di privacy.

Quanto pubblicato su un Social Network è persistente e non è facile da cancellare, bisogna evitare la pubblicazione di contenuti che in futuro non si vorrebbe veder pubblicati;

Quando si contribuisce con del materiale in un ambiente condiviso, l'utente è tenuto ad essere coerente con il contesto e le regole di fatto dalla community, evitando di pubblicare materiale inadeguato e che potrebbe risultare fuori contesto: ci sono momenti e luoghi virtuali per parlare di qualsiasi tema nel rispetto dei propri interlocutori.

Se si usa un nuovo servizio messo a disposizione dal Social Network, bisogna informarsi su quali sono gli strumenti per segnalare materiale e comportamenti non idonei, e quali sono le modalità corrette per farlo.

Se un contenuto viene moderato e non è più visibile online, probabilmente è non idoneo. Modificare linguaggio e controllare se il punto dove lo si è pubblicato è davvero il posto migliore per quello specifico contenuto.

Quando si fa uso di etichette per catalogare un contenuto/utente (TAG), bisogna assicurarsi che sia coerente con il contenuto o che indichi la persona corretta; quando il TAG riguarda una persona sarebbe inoltre opportuno contattarla preventivamente per ottenere il consenso a collegare l'identità della persona al contenuto.

La gestione delle relazioni sociali – Communities – (Rapporto N a N)

Le relazioni sociali che si sviluppano all'interno di un Social Network sono simili a quelle reali, deve essere gestita la fiducia verso i propri contatti proprio come accade nella realtà. Bisogna aggiungere alla propria rete di amici solo le persone che hanno in vari modi dimostrato di essere affidabili, con cui si è a proprio agio e di cui siamo a conoscenza della reale identità. Inoltre conviene gestire la propria privacy quando si aggiungono persone su cui si hanno dubbi o non si conoscono affatto.

Se si instaura un'amicizia virtuale con persone di cui non si conosce la reale identità, bisogna evitare di condividere contatti e dati personali e contenuti privati, soprattutto se riguardano terze persone.

La rete sociale non è facile da controllare quindi bisogna tenere sempre a mente che gli "amici degli amici" o di componenti del proprio "network" sono molti e spesso hanno modo, nonostante siano sconosciuti, di avere accesso alle informazioni e ai contenuti personali.

Se si ha accesso alle comunicazioni private di altri utenti, per esempio perché l'utente ha impostato in maniera sbagliata i livelli di privacy, bisogna notificarlo all'utente ed evitare di leggere i messaggi privati.

La reputazione digitale è persistente e si diffonde velocemente pertanto non bisogna mai diffamare altre persone, soprattutto se le stesse non sono presenti sul Social Network e non possono accorgersi del danno subito.

