

Istituto Comprensivo 1 Asti

P.U.A. (Politica d'Uso Accettabile e Sicura della rete) e uso consapevole delle T.I.C. (Tecnologie Informazione Comunicazione)

Premessa

Negli ultimi anni il nostro istituto si è dotato di attrezzature informatiche e multimediali di ultima generazione per consentire una modernizzazione delle attività formative, con metodologie e applicazioni di una didattica sostenuta dall'uso delle TIC. (Tecnologie di comunicazione informatica)

Tale dotazione tecnologia e multimediale ha dato un notevole impulso alla innovazione metodologica da parte dei docenti, favorendo e stimolando un'efficace ricaduta delle didattiche specifiche sui saperi, i saper fare, le competenze degli alunni. Infatti, oltre alle discipline che trattano specificamente il linguaggio informatico, anche le discipline tradizionali si avvalgono di "pacchetti" di programmi appositamente studiati per la didattica, per il recupero o il potenziamento, per supportare e facilitare l'apprendimento negli alunni con disabilità, favorendone l'integrazione.

Le nuove tecnologie costituiscono però anche una potenziale fonte di rischi, tanto più rilevanti quanto meno è diffusa una cultura relativa ai modi legittimi di usarla e alla consapevolezza delle funzioni che la Rete rende possibili. Ne siamo consapevoli e il nostro istituto è da tempo impegnato nell'educazione dei propri alunni ad un uso consapevole, positivo e responsabile delle tecnologie e della multimedialità.

C'è poi un altro aspetto da considerare e riguarda la rete interna dell'Istituto. Il suo uso improprio può generare disfunzioni da un punto di vista didattico, difficoltà di uso delle macchine, fino al blocco delle stesse, comportando un danno anche economico. E' prioritario quindi definire, all'interno della nostra istituzione scolastica, delle regole chiare che pongano le basi per lavorare serenamente, sicuri di aver messo in atto quanto possibile in chiave di prevenzione, ma soprattutto per usare in modo efficiente le suddette tecnologie.

La definizione della PUA di Istituto, spetta al Dirigente Scolastico, che si avvale del personale docente cui sono stati assegnati compiti specifici relativi all'infrastruttura tecnologica d'Istituto e alla sua sicurezza .

Il presente documento, parte integrante del Regolamento di Istituto, sarà portato a conoscenza dei genitori, degli allievi e notificato tramite pubblicazione sul sito a tutto il personale della scuola e da loro condiviso .

Nel documento che definisce la PUA d'Istituto sono definiti ordinamenti in merito a:

- ⊙ accesso alle postazioni in rete della scuola dei diversi soggetti operanti nell'Istituto: personale in servizio, allievi, eventuali soggetti esterni alla scuola;
- ⊙ accesso ai servizi resi disponibili sui computer in rete dei diversi soggetti operanti nell'Istituto;
- ⊙ garanzie a tutela della privacy nell'uso degli strumenti tecnologici d'Istituto.

CONTENUTI

1. I vantaggi di internet a Scuola
2. Accertamento dei rischi e valutazione dei contenuti di Internet
3. Strategie della Scuola per garantire la sicurezza delle TIC
4. Norme e linee guida
5. Indicazioni specifiche per gli alunni
6. Indicazioni specifiche per i docenti
7. Indicazioni specifiche per la segreteria
8. La gestione del sito della Scuola
9. Informazioni sulla PUA della Scuola
 1. Informazioni per gli studenti
 2. Informazioni per il personale scolastico
 3. Informazioni per i genitori/tutori

1. I vantaggi di Internet a scuola

La competenza digitale è inclusa tra le otto competenze chiave da assicurare nelle strategie di apprendimento per tutti i cittadini europei secondo le raccomandazioni delle istituzioni comunitarie (Consiglio dell'Unione Europea e del Parlamento Europeo - 2006/962/CE del 18 dicembre 2006). Le competenze chiave sono quelle di cui tutti hanno bisogno per la realizzazione e lo sviluppo personali, per la cittadinanza attiva, l'inclusione sociale e l'occupazione.

Internet deve essere presentato ed offerto, agli allievi e a tutta l'utenza scolastica, come un prezioso strumento per incentivare scambi culturali, per avviare progetti e per acquisire informazioni e documenti utili alle discipline scolastiche nell'ottica di una comune crescita culturale e formativa.

L'utilizzo della rete interna ed esterna (web) deve essere fatto nell'ambito della programmazione didattica (almeno nelle linee di fondo) e nell'ambito delle esigenze relative agli uffici amministrativi.

La scuola ha quindi il compito di attivare una vera e propria "alfabetizzazione informatica" in modo che per tutti Internet possa essere un diritto ed un privilegio.

Il docente, in primo luogo, ha la responsabilità di guidare gli studenti nelle attività online stabilendo obiettivi chiari di ricerca in Internet, insegnando le strategie appropriate nella definizione e gestione della risorsa informatica. Solo un utilizzo mirato e consapevole aiuta a garantire la massima sicurezza in informatica.

2. Accertamento dei rischi e valutazione dei contenuti di internet

La scuola si fa carico di tutte le precauzioni necessarie per garantire agli studenti l'accesso a materiale appropriato, anche se non è possibile evitare che gli studenti trovino materiale indesiderato navigando su un computer della scuola. La scuola non può farsi carico della responsabilità per il materiale trovato su internet o per eventuali conseguenze causate dall'accesso ad internet.

Gli studenti devono essere pienamente coscienti dei rischi a cui si espongono quando sono in rete.

Gli studenti devono imparare ad utilizzare i metodi di ricerca, che includono i cataloghi per soggetto e l'uso dei motori informatici.

L'utilizzo della posta elettronica tramite Internet è consentito solo se legato ad attività didattiche.

Nell'utilizzo di Internet è necessario seguire le seguenti precauzioni:

Attenzione alla validità nella diffusione e nell'origine delle informazioni a cui si accede.

Utilizzazione di fonti alternative di informazione per proposte comparate.

Rispetto dei diritti d'autore e dei diritti di proprietà intellettuale.

Attenzione ai rischi a cui gli studenti si espongono quando sono in rete.

Educazione al riconoscimento degli aspetti negativi di internet come la pornografia, la violenza, il razzismo e lo sfruttamento dei minori.

È inoltre necessario fare un breve ma importante riferimento ai rischi logici legati all'utilizzo degli archivi informatici, rischi che si riferiscono all'utilizzo di dati sensibili.

- ▶ Rischio interno relativo all'utilizzo della rete da parte di personale non autorizzato ad accedere ai dati.
- ▶ Rischio esterno relativo all'accesso ai dati da parte di persone estranee all'amministrazione attraverso gli eventuali punti di ingresso/uscita verso internet.
- ▶ Rischio esterno dovuto ad intrusioni nel sistema da parte di hacker/cracker.
- ▶ Rischio interno dovuto a intrusioni da parte di studenti.
- ▶ Rischio interno/esterno di scaricamento virus e/o trojan per mezzo di posta elettronica e/o operazioni di download eseguite tramite il browser.

3. Strategie della scuola per garantire la sicurezza delle TIC

Separazione della rete didattica dalla rete amministrativa.

La rete amministrativa è dotata, a norma di legge, di un software che traccia tutti gli accessi fisici al server.

L'utilizzo dei laboratori di informatica è regolamentato da un apposito orario; il docente firma la presenza e segnala tempestivamente eventuali anomalie; gli alunni possono accedere solo se accompagnati da docenti.

Il sistema informatico delle TIC della Scuola viene regolarmente controllato, per prevenire, ed eventualmente rimediare, possibili disfunzioni dell'hardware o del software dal Referente TIC addetto della rete.

È vietato inserire file sul server/teacher o scaricare software da internet non autorizzati.

I laboratori informatici sono "a profili bloccati": gli alunni non possono modificare le impostazioni dei singoli PC.

La password per l'accesso wireless verrà data esclusivamente ai docenti che ne faranno richiesta. Gli allievi non potranno usufruire dell'accesso wireless.

Utilità di sistema e file eseguibili, reperibili su supporti provenienti da riviste o altro, non possono essere configurati.

In generale il software utilizzabile è solamente quello autorizzato dalla Scuola.

4. Norme e linee guida

Tutti gli utenti connessi ad internet devono rispettare:

- ❖ la legislazione vigente applicata anche alla comunicazione su internet;
- ❖ la netiquette (etica, galateo e norme di buon uso dei servizi di rete);
- ❖ dopo un certo numero di violazioni delle regole stabilite dalla politica scolastica, la Scuola ha il diritto di interdire l'accesso dell'utente a internet per un certo periodo di tempo o in modo permanente;

Il sistema di accesso ad internet della scuola prevede l'uso di un filtro (DansGuardian con funzioni di filtro dei contenuti) per impedire l'accesso a contenuti non compatibili con la politica educativa della scuola (sesso, violenza, droghe, comportamenti criminali, occultismo, appuntamenti ed incontri, giochi d'azzardo, ecc.).

Si specifica che il filtro non si limita a controllare una lista di siti proibiti, bensì agisce sui contenuti delle pagine web. Il proxy registra tutte le richieste internet.

Ogni laboratorio è dotato del software Italc: controlla e interagisce in tempo reale con tutti i computer.

❖ il Referente TIC controllerà settimanalmente l'efficacia del sistema di filtraggio;

❖ la Scuola riferisce alle autorità competenti se è stato trovato materiale illegale.

5. Indicazioni specifiche per gli alunni

- ⊗ L'accesso agli strumenti informatici avviene esclusivamente con la supervisione dei docenti.
- ⊗ Occorre l'autorizzazione dell'insegnante per scaricare documenti da internet.
- ⊗ Non è consentito l'uso di pen- driver o dvd personali senza specifica autorizzazione.
- ⊗ Non è consentito utilizzare materiale per le esercitazioni che non sia stato controllato dal docente.
- ⊗ Gli alunni sono tenuti al rispetto delle attrezzature, dei pacchetti applicativi e delle norme di archiviazione dei dati.
- ⊗ Non è consentito utilizzare applicazioni di messaggistica istantanea e social network.
- ⊗ Non è consentito utilizzare giochi né in locale, né in rete;
- ⊗ Occorre riferire all'insegnante ogni malfunzionamento riscontrato.
- ⊗ Occorre riferire all'insegnante di eventuali messaggi o immagini illecite o inadeguate.
- ⊗ Salvate sempre i vostri lavori (file) in cartelle personali e/o di classe indicate dal referente TIC e non sul desktop o nella cartella del programma in uso.

6. Indicazioni specifiche per i docenti

- ⊗ Deve essere garantita una costante supervisione sull'uso di tutte le tecnologie da parte degli alunni.
- ⊗ Per l'utilizzo dei laboratori di informatica è richiesto agli insegnanti di seguire le indicazioni del docente referente e di collaborare per un uso responsabile e corretto degli strumenti e del materiale.
- ⊗ Durante le proprie ore di utilizzo del laboratorio, il docente si assume tutte le responsabilità per il download di materiale e la visita di siti non connessi all'attività didattica.
- ⊗ E' bene discutere con gli studenti del Regolamento della scuola e degli eventuali problemi che possono verificarsi nell'applicazione delle regole relative all'uso di internet.
- ⊗ E' compito dell'insegnante vigilare affinché l'accesso alle macchine avvenga in modo ordinato, l'utilizzo e lo spegnimento in modo corretto, a garanzia della sicurezza di tutti gli utenti.
- ⊗ Eventuali guasti devono essere tempestivamente segnalati al referente di laboratorio.
- ⊗ La stampa dei documenti da parte delle classi e degli alunni è consentita solo nei limiti della disponibilità di risorse indicate dal dirigente scolastico.
- ⊗ Eventuali docenti esterni autorizzati all'utilizzo del laboratorio devono farsi carico dell'intera applicazione del presente Regolamento.
- ⊗ Evitate di lasciare le e-mail o file personali sui computer o sul server della scuola
- ⊗ Salvate sempre i vostri lavori (file) in cartelle personali e/o di classe indicate dal referente TIC e non sul desktop o nella cartella del programma in uso.

7. Indicazioni specifiche per la segreteria

- ⊗ Il personale di segreteria tratta i dati conservati nel sistema informatico con utilizzo di password da rimuovere ogni sei mesi (tre in caso di dati sensibili).
- ⊗ Le password di accesso sono personali e non devono essere comunicate ad altre persone al di fuori del responsabile del trattamento dei dati e del responsabile della sicurezza informatica.
- ⊗ Al termine di ogni settimana di servizio deve essere effettuato il backup dei dati e devono essere custodite le copie in luogo sicuro e ad accesso controllato.
- ⊗ Su tutte le postazioni deve essere controllata la validità del sistema antivirus con gli opportuni aggiornamenti.

8. Gestione del sito web della scuola

Il Webmaster gestisce le pagine del sito ed è sua responsabilità garantire che il contenuto sia accurato e appropriato.

E' tenuto a rispettare le linee guida sulle pubblicazioni della Scuola.

Questa detiene i diritti d'autore dei documenti pubblicati.

Le informazioni editate nel sito, relative alle persone da contattare, devono includere solo l'indirizzo della scuola, l'indirizzo di posta elettronica e il telefono della scuola, ma non notizie relative agli indirizzi del personale o altre informazioni del genere.

Il sito Web potrà solo pubblicare tutto ciò che, nella prassi comune, può essere affisso sulle bacheche e all'interno della Scuola.

Il presente regolamento interno PUA sarà reso pubblico attraverso il sito Web della scuola e disponibile presso i laboratori informatici.

9. Informazione sulla politica d'uso accettabile della scuola (PUA)

9.1 INFORMARE GLI STUDENTI

Le regole di base relative all'accesso ad internet verranno esposte nei laboratori di informatica. Gli studenti saranno informati che l'utilizzo del web è monitorato e verranno loro date delle istruzioni per un uso responsabile e sicuro; queste regole appropriate ed elaborate per un Uso Accettabile e Responsabile della Rete sono indirizzate alle scuole di base e alla scuola secondaria di primo grado.

Gli studenti e i loro genitori/tutori devono firmare il documento per presa visione.

9.2 INFORMARE IL PERSONALE SCOLASTICO

Il personale scolastico e i docenti avranno una comunicazione in merito alla pubblicazione sul sito della Politica d'Uso Accettabile della rete, che sarà così notificata, ed è consapevole che l'uso di internet verrà monitorato e segnalato e tutto il personale scolastico sarà coinvolto nello sviluppo delle linee guida della Politica d'Uso Accettabile della rete e nell'applicazione delle istruzioni sull'uso sicuro e responsabile della rete come richiesto.

In caso di dubbi legati alla legittimità di una certa istanza utilizzata in internet, l'insegnante dovrà contattare il Dirigente scolastico o la commissione per la PUA per evitare malintesi.

9.3 INFORMARE I GENITORI/TUTORI

I Genitori vengono informati della pubblicazione della PUA, unitamente al documento che regola l'Uso Accettabile e Responsabile di internet, sul sito WEB della Scuola e presso la Segreteria. Verranno inoltre informati su di una serie di regole da seguire a casa.

Eventuali commenti o suggerimenti connessi alla Politica d'Uso Accettabile possono essere inviati al responsabile delle TIC.

La Scuola deve chiedere ai genitori il consenso all'uso di internet per il loro figlio o per la pubblicazione dei suoi lavori e delle sue fotografie.

Garanzie a tutela della privacy

Tutte le operazioni relative all'uso della "rete" sono improntate alla tutela della "privacy".

Relativamente alla "tutela della persona ed di altri soggetti, rispetto al trattamento dei dati personali", verrà data la prevista informativa. La titolarità è esercitata dal Dirigente Scolastico. Il Dirigente scolastico designa il responsabile del trattamento dei dati, che coincide con la figura del Direttore SGA. e segreterie delle Istituzioni Scolastiche devono dotarsi di "misure minime", di "strumenti" e "amministratori di sistema", secondo quanto previsto dal D.P.R.318/1999, precisamente:

"misure minime", adozione di password; individuazione dei soggetti preposti alla gestione delle password; adozione di un codice identificativo personale per ogni utente; adozione di programmi antivirus; protezione e regolamentazione degli accessi ai locali che ospitano i dati riservati o in cui si trovano le postazioni di lavoro che ne consentono l'accesso; i criteri per garantire l'integrità dei dati; i criteri per garantire la trasmissione sicura dei dati; "strumenti", adozione di mezzi elettronici adeguati per impedire l'accesso dall'esterno alla rete della segreteria, quali FIREWALL od altri strumenti; "amministratori di sistema" il Direttore SGA, cui è conferito dal Dirigente il compito di sovrintendere al sistema di gestione e custodia dei dati personali, individua gli incaricati del trattamento dei dati medesimi e ne indica i criteri di gestione, attribuendo a ciascun incaricato un codice identificativo personale per l'utilizzazione dell'elaboratore.

E' da prevedere un piano di formazione e di aggiornamento degli incaricati del trattamento dei dati sui rischi di distruzione o perdita dei dati e sulle contromisure da adottare.

E' predisposto ed aggiornato, con cadenza annuale, un documento programmatico sulla sicurezza dati per definire i criteri tecnici ed organizzativi per la protezione dei locali e degli elaboratori in cui sono custoditi i dati e le procedure per assicurarne l'integrità.

Asti, 8/9/2017