ISTITUTO COMPRENSIVO STATALE
Ciminna
Via Trieste, 25
90023 Ciminna
Cod. Fiscale 97169260821

REGOLAMENTO PER L'USO DELLE TECNOLOGIE INFORMATICHE E DELLA COMUNICAZIONE

Approvato con deliberazione n. 64 del Consiglio di Istituto del 27/03/2018

REGOLAMENTO PER L'USO DELLE TECNOLOGIE INFORMATICHE E DELLA COMINICAZIONE
P.U.A. - Politica d'Uso Accettabile e Sicura della Scuola

Premessa

Entrando in internet si accede ad una grande quantità di dati messi a disposizione spesse volte gratuitamente da altri utenti. Pertanto è doveroso portare rispetto verso quanti hanno prestato e prestano opera per consentire a tutti di utilizzare un grande patrimonio di informazioni continuamente in crescita che, altrimenti, soltanto pochi o addirittura singoli potrebbero beneficiare.

In Internet regna un disordine ordinato in quanto non esiste una autorità centrale che regolamenti cosa si può fare e cosa no, né esistono organi di vigilanza. E' infatti demandato alla responsabilità individuale il buon funzionamento delle cose. Si può, pertanto, decidere di entrare in Internet come persone civili, o al contrario, si può utilizzare la rete comportandosi da predatori o vandali saccheggiando le risorse presenti in essa o peggio per perpetuare attività criminose. Sta a ciascuno decidere come comportarsi e quali obiettivi vuole raggiungere nell'utilizzo di internet.

Risulta, così, chiaro come le cose potranno continuare a funzionare solo in presenza di una consapevole autodisciplina.

L'Istituto comprensivo Ciminna pertanto, su indicazione delle linee guida contenute nella lettera circolare n. 14 del MIUR del 24/10/2002 unitamente alla C.R. 142/2003, a quanto reperibile di pertinente nel sito istituzionale www.istruzione.it/innovazione/tecnologie/consapevole.shtml, ed infine, quanto di utile è stato rintracciato nel sito dell'European Schoolnet (organismo promosso dall'EU per la cooperazione tra i Ministeri dell'Istruzione dei Paesi dell'Unione Europea per l'uso didattico delle ICT, in raccordo con i network educativi europei nazionali, regionali e locali), elabora il presente Regolamento, periodicamente revisionabile, relativo alla Politica d'Uso Accettabile delle Tecnologie dell'Informazione e della Comunicazione. Il presente Regolamento, che definisce l'aspetto della Policy d'Istituto che è da intendere come le *"regole condivise per l'uso della rete locale e dei servizi su di essa attivati"*, intende conseguire i seguenti obiettivi:

1. I vantaggi di internet a scuola;
2. Accertamento dei rischi e valutazione dei contenuti di internet;
3. Le strategie della scuola per garantire la sicurezza delle TIC (Tecnologie dell'Informazione e della Comunicazione);
4. Norme e linee guida;
5. Fornitore di servizi internet;
6. Mailing list moderate, gruppi di discussione e chat room;
7. Uso delle immagini e dei filmati nella scuola;
8. Gestione del sito web della scuola;
9. Informazioni sulla Politica d'Uso Accettabile della scuola.

Lo scopo del presente documento è quello di garantire un uso corretto e responsabile delle apparecchiature informatiche in dotazione all'Istituto Comprensivo Ciminna nel rispetto delle norme vigenti.
E' altrettanto evidente che le regole approvate nel presente disciplinare tecnico devono avere una valenza formativa, e non solo sanzionatoria, perché il loro scopo è quello di aiutare gli utenti meno esperti a orientarsi in merito a temi quali la privacy, la libertà di espressione, il plagio, la identificazione ed identità di rete, l'etica nella rete, i vincoli legali, le molestie, l'utilizzo delle risorse, il rispetto verso gli altri.

1) -I vantaggi di Internet a Scuola

Il curricolo scolastico prevede che gli studenti imparino ad utilizzare le ICT (Information and Communication Technology) per approfondire le conoscenze, recuperare documenti e scambiare informazioni. Internet offre a tutti una vasta scelta di risorse e opportunità culturali, sociali, scolastiche e per il tempo libero. La scuola oggi propone l'utilizzo di internet per promuovere il successo formativo, per tendere all'eccellenza in ambito didattico, attraverso la condivisione delle risorse, l'innovazione e la comunicazione.

Per gli studenti come per i docenti e per tutti gli operatori scolastici l'accesso ad internet non è solo un privilegio ma è soprattutto un diritto.

Durante la consultazione esiste la reale possibilità di trovare materiale inadeguato ed anche illegale per cui la scuola adotterà, seguendo l'evoluzione dei sistemi, tutti i mezzi e i software atti a difendere l'accesso da parte degli alunni a quei siti ritenuti pericolosi.

Resta fondamentale il ruolo degli insegnanti che hanno la responsabilità di guidare gli studenti nelle attività on line, di stabilire obiettivi chiari per un uso consapevole di Internet, di prevenire il verificarsi di situazioni critiche, utilizzando percorsi guidati e controllati.

L'obiettivo principale resta quello di arricchire ed ampliare le attività didattiche, secondo quanto previsto dal curricolo scolastico in base all'età e alla maturità dei discenti.

Più in particolare:

Internet per il personale scolastico

Per quanto riguarda il personale docente l'accesso ad internet consente di svolgere in modo agevole ed efficace svariate funzioni professionalmente rilevanti, prima tra tutte l'autoaggiornamento e la partecipazione ad iniziative di e-learning.

Essendo l'esigenza dell'aggiornamento una priorità proprio nel campo stesso del corretto ed efficace uso delle nuove tecnologie per la didattica, la possibilità di accedere da scuola alle risorse documentarie tramite Internet diviene un fattore imprendiscibile per lo svolgimento della professionalità del personale ATA e docente.

Internet per gli allievi

Un monitoraggio svolto dal Ministero della Pubblica istruzione indica come la scuola sia l'ultimo dei luoghi in cui i ragazzi in età dell'obbligo scolastico hanno occasione di connettersi a internet. Il dato può apparire rassicurante dal punto di vista della tutela dei minori verso l'esposizione ai rischi della rete, ma anche preoccupante per il mancato ruolo di guida che la scuola dovrebbe svolgere verso gli alunni e le famiglie.

Sempre maggiori appelli vengono rivolti alla scuola su questo fronte. Infatti l'accesso alle risorse informative e documentarie e ai servizi di ricerca on-line appaiono sempre più vicini agli specifici compiti culturali della scuola. La funzione di internet quale "strumento" di accesso al sapere al fianco degli strumenti tradizionali lo rende implicitamente oggetto di attenzione per la formazione dei giovani. In tal senso in diversi documenti del MIUR l'approccio all'informatica e alla telematica vengono presentati come ambiti formativi non solo disciplinari, ma trasversali all'azione educativa che la scuola svolge.

2) - Accertamento dei rischi e valutazione dei contenuti di Internet

La scuola metterà in atto tutte le azioni necessarie per garantire agli studenti l'accesso alla documentazione cercata, anche se non è possibile assicurare una navigazione totalmente priva di rischi. La scuola non può farsi carico della responsabilità per il materiale trovato su Internet e per eventuali conseguenze causate dall'accesso accidentale a siti illeciti. Tuttavia è dovere della scuola garantire il Diritto dei minori in rete e adottare tutti i sistemi di sicurezza conosciuti per diminuire le possibilità di rischio durante la navigazione.

Con Internet gli studenti imparano ad utilizzare metodi di consultazione e motori di ricerca. Ricevere ed inviare messaggi con allegati via e-mail è conseguenza del possesso di una buona abilità nella gestione delle informazioni e della comunicazione. Tale abilità include:

- un controllo della validità e dell'origine delle informazioni a cui si accede o che si ricevono;
- un utilizzo di fonti alternative di informazione per proposte comparate;
- una ricerca del nome dell'autore, dell'ultimo aggiornamento del materiale e dei possibili altri link al sito;
- un rispetto dei diritti d'autore e dei diritti di proprietà intellettuale.

E' utile riportare in questa sezione, anche se brevemente, l'esistenza degli *smartphone e tablet* e i rischi che connessi nel loro quotidiano utilizzo: il riferimento è unitamente collegato anche al *cloud computing,* argomento presentato nel punto 5) del presente regolamento.

Gli *smartphone* - o cellulare intelligente o telefono *touch* , cioè sensibile al tocco – è un dispositivo portatile, alimentato a batteria, che coniuga le funzionalità di telefono cellulare con quelle di elaborazione e trasmissione dati tipiche del mondo dei personal computer; esso, inoltre, impiega sensori per la determinazione della posizione (GPS) e per l'acquisizione di altri elementi dell'ambiente circostante l'utente.

Le componenti *hardware* generalmente presenti in dispositivi di questo genere sono riassunte nella Tab. 1, mentre le caratteristiche funzionali e la tipologia d'uso sono descritte in Tab. 2:

Componenti trasmissive	Sensori e dispositivi
Modulo telefonico	Schermo *touch* inferiore a 5''
Wifi (rete senza fili)	Altoparlante e microfono integrati
Bluetooth (rete senza fili)	Fotocamera/videocamera digitale
Radio FM	Dispositivo di localizzazione (GPS)
	Bussola digitale e altri sensori
	Moduli di pagamento

Tab. 1 – Smartphone: caratteristiche + hardware di massima

Nuove caratteristiche
Applicazioni con funzionalità di localizzazione
Riconoscimento vocale, facciale e di immagini
Social network con possibilità di rendere nota la posizione geografica degli utenti
L'utente generalmente acquisisce applicazioni utilizzando lo specifico market dedicato (*Ovistore*, per *Nokia*, *Apple Store*, *Android Market* per *Google*, *Windows Market Place* per *Microsoft*)
Possibilità di confusione tra dati di origine diversa (es. quelli contenuti nella rubrica per uso personale e quelli relativi ai contatti di lavoro)

Tab. 2 – Smartphone: applicazioni innovative e nuove funzionalità delle applicazioni tradizionali

I *tablet* o *tablet computer* sono dispositivi assimilabili per componenti hardware e software agli *smartphone*, dai quali si distinguono per:

- Dimensioni dello schermo;
- Possibile assenza del modulo telefonico;
- Destinazione d'uso.

Gli utenti tendono a delegare la gestione di molti aspetti della propria vita sia personale che professionale alle nuove tecnologie, le quali fanno sempre più spesso impiego di informazioni relative alla geolocalizzazione degli interessati. Questi dati non sempre restano archiviati esclusivamente sul dispositivo, ma vengono frequentemente conservati in aree remote potenzialmente accessibili anche da altri utenti. Uno stesso *smartphone* può essere utilizzato per finalità più disparate, ad esempio per la gestione del *portoflio* clienti, del catalogo e del calendario aziendali, ma anche per la condivisione di foto, informazioni, video, etc. con i propri familiari o amici, per il confronto dei prezzi dei prodotti al supermercato con quelli del negozio *on-line,* per monitorare i propri movimenti bancari, per localizzare la propria automobile in caso si dimentichi dove è stata parcheggiata, per sapere, in quel determinato momento, chi dei propri amici si trova in zona, per redigere programmi di benessere alla stregua delle proprie abitudini alimentari, per impostare il monitoraggio ormonale del ciclo femminile, e magari, in una prospettiva di prossima, futura realizzazione, persino come telecomando per aprire il cancello automatico del proprio box auto o per bloccare la serratura della propria abitazione. Il ventaglio delle applicazioni possibili è allora, realmente impressionante e destinato ad accrescersi ulteriormente. Tuttavia, l'utilizzo di tali applicazioni implica l'elaborazione e quindi il trattamento dei dati, anche personali, riservati e persino sensibili. In molti casi i dati verranno archiviati e conservati sul dispositivo, ma sempre più spesso ci si avvale di *mobile apps (software* che è possibile installare sugli *smartphone* e sui *tablet* per fornire

funzionalità aggiuntive) che consistono realmente in servizi erogati in modalità *web,* il cui utilizzo implica, cioè, che le informazioni personali siano spostate o copiate nella *cloud* del fornitore del servizio. Il fornitore, ovvero lo sviluppatore delle *mobile apps*, può essere lo stesso gestore del market o uno sviluppatore indipendente. In altri termini molte delle applicazioni per *smartphone* sono servizi erogati in modalità *cloud* che trasportano tutti o parte dei dati dell'utente nella *cloud*.

Si apre uno scenario nuovo ed impensabile sui rischi e minacce specifici i cui fattori sono connessi all'utilizzo dei sistemi *mobile* idonei a determinare, appunto, rischi e minacce per la protezione dei dati personali degli utenti. In particolare:

- La linea di demarcazione tra *l'identità digitale* dall'*identità reale* tende progressivamente ad affievolirsi sino a scomparire;
- Il *social networking* tende ad essere sempre più pervasivo e si integra e arricchisce con nuove informazioni personali (ad es. la posizione geografica dell'utente);
- In generale, a causa dell'integrazione dei servizi informatici e dello scambio di dati tra applicazioni, telefono e servizi, è sempre più difficile – e spesso impossibile – controllare il flusso dei propri dati personali;
- A causa della progressiva diminuzione del controllo sui propri dati e della correlata fusione tra l'identità digitale e quella reale, emergono maggiori pericoli dal punto di vista della sicurezza informatica e si creano nuovi rischi e minacce (ad esempio *stalking* sociale, intercettazioni, furto di *account* di pagamento);
- Possibilità di accedere da parte delle applicazioni a dati e strumenti in modo ancor più invasivo che in passato (numero telefonico, rubrica, messaggi);
- Possibilità da parte delle applicazioni di intrecciare aspetti differenti della vita degli utenti (es. vita privata e vita professionale) in modi non sempre chiari, conoscibili, prevedibili, controllabili e desiderati da parte dell'utente stesso;
- Tracciamento e profilazione dell'utente a sua insaputa e disponibilità di dati univoci da utilizzare ad esempio per la pubblicità comportamentale o per la tutela del diritto d'autore;
- Alcuni produttori, per ragioni di mercato, tendono a non distribuire tempestivamente gli aggiornamenti software che risolvono accertate vulnerabilità di sicurezza informatica.

Non è possibile tralasciare di dare utili informazioni sull'utilizzo delle app. Infatti, milioni di persone utilizzano e installano ogni giorno su smartphone e tablet diversi tipi di app per comunicare, giocare, dare sfogo alla creatività, ma anche per studiare e lavorare. Si tratta di strumenti divertenti, utili, in alcuni casi divenuti indispensabili alla nostra vita quotidiana.

E' bene ricordare però che le app possono raccogliere e trattare una grande quantità di dati personali, a volte anche di natura sensibile. Basti pensare che le app possono avere accesso alla rubrica dei contatti, a foto, video e documenti di vario tipo, ai dati della carta di credito o magari anche al microfono dello smartphone o del tablet. Ma possono anche registrare informazioni sulle abitudini di vita, sui consumi, sulla posizione geografica e perfino sulla forma fisica e sullo stato di salute.

E' quindi importante scegliere e usare le app in maniera consapevole, in modo tale da conoscerne le opportunità, ma anche gli eventuali rischi per la nostra privacy.

Per sensibilizzare gli utenti italiani, il Garante per la protezione dei dati personali lancia una campagna informativa attraverso un video tutorial e una scheda informativa, realizzati con l'obiettivo di offrire alcune semplici e utili indicazioni di base su come tutelare la propria *privacy* quando si scaricano applicazioni, specialmente quando ad usarle sono dei minori.

Il video di animazione predisposto dal Garante *Privacy*, intitolato "*APP-prova di privacy*", rivolto in particolare ad un pubblico giovane, può essere scaricato dal sito web dell'Autorità all'indirizzo **www.garanteprivacy.it/app**, oppure visto in *streaming* sul canale *Youtube* **http://www.youtube.com/videogaranteprivacy** e sugli altri profili social del Garante come **Linkedin** e **Google+**.

Gli studenti devono essere pienamente consapevoli dei rischi a cui si espongono e spingono terzi quando si naviga in rete e in mobile. Essi devono essere educati a riconoscere e ad evitare gli assetti negativi di internet (pornografia, violenza, razzismo, sfruttamento dei minori ed ancora altri eventi) e, qualora ne venissero a contatto, devono riferire immediatamente il fatto all'insegnante o al docente responsabile del laboratorio.

3) - Strategie della scuola per garantire la sicurezza delle ICT

Ogni sede avrà un responsabile di laboratorio nominato dal Collegio dei docenti al quale gli altri operatori dovranno rivolgersi.

Ogni collaboratore sarà tenuto a leggere, conoscere e sottoscrivere il presente disciplinare tecnico, impegnandosi a prendere piena consapevolezza delle responsabilità di propria competenza.
E' consentito l'accesso alle postazioni dei computer negli orari di apertura della scuola per compiti connessi allo svolgimento delle proprie mansioni. Le attività dei laboratori sono regolamentati da orari di apertura e di chiusura.
E' consentito l'accesso agli alunni in orario scolastico solo ed esclusivamente se accompagnati dal docente di riferimento, il quale controllerà che l'utilizzo avvenga secondo le modalità previste dal presente regolamento. Ogni plesso predisporrà un calendario di utilizzo dei laboratori.

Le strategie previste da adottare sono:

- Regolamentazione, tramite orario settimanale, dell'utilizzo di laboratori di informatica a cui gli alunni possono accedere solo se accompagnati dai docenti, i quali sono responsabili di quanto avviene nelle proprie ore di laboratorio;
- Indispensabilità della separazione fisica della rete didattica da quella amministrativa;
- Utilizzo di password di sistema per attivare l'accesso ai computer;
- Controllo del sistema informatico della scuola al fine di prevenire e/o rimediare a possibili disfunzioni dell'hardware o del software;
- Regolare periodicità del controllo, da parte dei docenti facenti parte della commissione informatica, dei file utilizzati, di quelli temporanei, dei siti visitati e della cronologia;
- E' fatto divieto di accedere a risorse di rete internet o esterne alla scuola;
- E' fatto divieto di cancellare, disinstallare, copiare o asportare deliberatamente programmi software per scopi personali o per altri motivi non pertinenti alle attività didattiche;

- E' fatto divieto di rimuovere, danneggiare deliberatamente o asportare componenti hardware;
- Abbandonare il posto di lavoro lasciandolo incustodito e quindi accessibile ad altri operatori, se non con l'autorizzazione del docente presente in aula;
- E' fatto divieto di inserire file sul server o scaricare software non autorizzati;
- Utilizzo di un software antivirus aggiornato costantemente;
- Utilizzo di CD personali e di chiavette previa autorizzazione di un docente facente parte della commissione informatica, che li sottopone ad un controllo antivirus;
- Possibilità di utilizzare solo software autorizzati dalla scuola;
- Controllo periodico dello spazio web dedicato alle attività didattiche della scuola;
- E' fatto divieto assoluto di modificare le impostazioni di sistema trovate in uso: desktop, screensever, …..

La scuola, per opportunità nascenti da organizzazione interna delle, potrà installare il sistema di comunicazione di tipo Skype così da godere di rapide e gratuite telefonate tra la sede centrale e i plessi dislocati in località diverse ed anche distanti.

4) – Cloud computing: indicazioni per un uso consapevole dei servizi

L'Autorità Garante per la Privacy, nell'ottica di promuovere un utilizzo corretto delle nuove modalità di erogazione dei servizi informatici, specie per quelli erogati tramite *cloud* pubbliche che comportano le esternalizzazione di dati e documenti, ritiene opportuna a doverosa un'opera di informazione orientata a tutelare l'importante patrimonio informativo costituito dai dati personali.

Quanto decritto in questo punto è tratto dalla Relazione annuale che l'Autorità ha presentato al Parlamento Italiano del mese di giugno 2011 e si ritiene di grande importanza sia per i nuovi servizi che Internet offre a tulle le Amministrazioni grandi e piccole, privati e pubblici.

Le indicazioni che saranno proposte hanno come obiettivo di offrire un primo insieme di indicazioni utili a tutti gli utenti di dimensioni contenute e di limitare risorse economiche destinatari delle crescente offerta di servizi di *cloud computing* con l'obiettivo di favorire l'adozione consapevole e responsabile di tali tipologie di servizi.

L'evoluzione delle tecnologie informatiche e dei mezzi di comunicazione è inarrestabile e ogni giorno vengono messi a disposizione dei cittadini nuovi strumenti e soluzioni sempre più sofisticate e integrate con la rete Internet, che consentono di soddisfare crescenti esigenze di informatizzazione e di comunicazione.

Il tale quadro il *cloud computing* è un insieme di modelli di servizio che più di altri si sta diffondendo con grande rapidità tra imprese, pubbliche amministrazioni e cittadini perché incoraggia un utilizzo flessibile delle proprie risorse (infrastrutture e applicazioni) o di quelle messe a disposizione da un fornitore di servizi specializzato. L'innovazione e il successo delle *cloud* (le nuvole informatiche) risiede nel fatto che, grazie alla raggiunta maturità delle tecnologie che ne costituiscono la base, tali risorse sono facilmente configurabili e accessibili via rete, e sono caratterizzate da particolare agilità di fruizione che, da una parte semplifica significativamente il dimensionamento iniziale dei sistemi e delle applicazioni mentre, dall'altra, permette di sostenere gradualmente lo sforzo di investimento richiesto per gli opportuni adeguamenti tecnologici e l'erogazione dei nuovi servizi.

Nell'ambito del *cloud computing* è ormai pressi consolidata distinguere tra *private cloud e pubblic cloud.*

Una *private cloud* (o nuvola privata) è un'infrastruttura informatica per lo più dedicata alle esigenze di una singola organizzazione, ubicata nei suoi locali o affidata in gestione ad un terzo nei confronti del quale il titolare dei dati può spesso esercitare un controllo puntuale.
Nel caso delle *pubblic cloud,* invece, l'infrastruttura è di proprietà di un fornitore specializzato nell'erogazione di servizi che mette a disposizione di utenti, aziende o amministrazioni – e quindi condivise tra di essi – i propri sistemi attraverso l'erogazione via web di applicazioni informatiche, di capacità elaborativi e di stoccaggio. La fruizione di tali servizi viene tramite la rete Internet e implica il trasferimento dell'elaborazione o dei soli dati presso i sistemi del fornitore del servizio, il quale assume un ruolo importante in ordine all'efficacia delle misure tecnologiche adottate per garantire la protezione dei dati che gli vengono affidati. In questo caso l'utente insieme ai dati, infatti, cede una parte importante del controllo esercitatile su di essi.
Acquisire servizi *cloud* significa acquistare presso un fornitore di servizio risorse (ad esempio server virtuali o spazio disco) oppure applicazioni(ad esempio posta elettronica e strumenti per l'ufficio).

- I dati non risiedono più sui server fisici dell'utente, ma sono allocati sui sistemi del fornitore (a meno di copie in locale)
- L'infrastruttura del fornitore del servizio è condivisa tra molti utenti per cui sono fondamentali adeguati livelli di sicurezza
- L'utilizzo del servizio avviene via web tramite la rete Internet che assume dunque un ruolo centrale in merito alla qualità dei servizi fruiti ed erogati
- I servizi acquisibili presso il fornitore del servizio sono a consumo e in genere è facile far fronte ad eventuali esigenze aggiuntive (ad esempio più spazio disco o più potenza elaborativi)
- Esternalizzare i dati in remoto non equivale ad averli sui propri sistemi: oltre ai vantaggi ci sono delle controindicazioni che bisogna conoscere.

Infine, per il momento, sul mercato, a seconda delle esigenze dell'utente, sono disponibili varie soluzioni di *cloud computing* erogate secondo modalità che ricadono in linea di massima in tre categorie, dette "modelli di servizio". Comunemente tali modelli di servizio sono riferiti sia a soluzioni di *private cloud* che di *pubblic cloud*, ma vengono illustrati in un'ottica maggiormente aderente a quest'ultima tipologia di servizi, che prevede l'utilizzo condiviso da parte di utenti, imprese e soggetti pubblici dei sistemi di provider di servizi terzi.

1. Nel caso di servizi *IaaS* (*Cloud Infrastructure as a Service* – Infrastruttura *cloud* resa disponibile come servizio)*,* il fornitore noleggia un'infrastruttura tecnologica, cioè server virtuali remoti che l'utente finale può utilizzare con tecniche e modalità che ne rendono semplice, efficace e produttiva la sostituzione o l'affiancamento ai sistemi già presenti nei locali dell'azienda.
2. Nel caso di *SaaS* (*Cloud Software as a Service* – software erogato come servizio della *cloud*), il fornitore eroga via web una serie di servizi applicativi ponendoli a disposizione degli utenti finali. Tali servizi sono spesso offerti in sostituzione delle tradizionali applicazioni installate localmente dall'utente sui propri sistemi ed è quindi spinto alla esternalizzazione dei suoi dati affidandoli al fornitore.
3. Nel caso di *PaaS* (*Cloud platform as a Service* – piattaforme sostare fornite via web come servizio) il fornitore offre soluzioni per lo sviluppo di hosting evoluto di applicazioni. In genere questo tipo di servizi è rivolto a operatori di mercato che li utilizzano per

sviluppare e ospitare soluzioni applicative proprie, allo scopo di assolvere a esigenze interne oppure per fornire a loro volta servizi a terzi.

Il fascino delle nuove tecnologie non deve far allontanare gli utenti finali dai potenziali rischi che i nuovi servizi web presentano. E' opportuno ricordare che l'innovazione impone il governo e la corretta gestione dei rischi. Occorre, cioè:

- Ponderare prioritariamente rischi e benefici dei servizi offerti;
- Effettuare una verifica in ordine all'affidabilità del fornitore;
- Privilegiare i servizi che favoriscono la portabilità dei dati;
- Assicurarsi la disponibilità dei dati in caso di necessità;
- Selezionare i dati da inserire nella *cloud;*
- Non perdere di vista i dati;
- Informarsi su dove risiederanno, concretamente, i dati
- Porre grande attenzione alle clausole contrattuali;
- Esigere ed adottare opportune cautele per tutelare la confidenzialità dei dati;
- Formare adeguatamente il personale

5) - Norme e linee guida

Tutti gli operatori connessi ad internet devono rispettare la legislazione vigente applicata alla comunicazione su Internet. Il sistema di accesso ad Internet della scuola deve prevedere l'uso di un filtro:

- che non deve permettere l'accesso a siti o pagine web incompatibili con la politica educativa della scuola (violenza, droghe, sesso, razzismo, etc.);
- che deve consentire solo l'accesso a un numero limitato di siti già selezionati;
- che non deve consentire le ricerche di pagine o siti web con l'uso di parole chiave inappropriate;
- che deve utilizzare un sistema di valutazione per la selezione di contenuti inadeguato attraverso l'uso di browser che respingono queste pagine;
- che deve monitorare i siti visitati dagli alunni e dagli insegnanti.

Hanno diritto ad accedere i dipendenti, le ditte fornitrici di software per motivi di manutenzione e limitatamente alle applicazioni di loro competenza, collaboratori nonché esperti esterni, impegnati nelle attività istituzionali per il periodo della collaborazione o contrattuale.

Qualora si registrasse un certo numero di violazioni delle regole stabilite dalla policy scolastica, la scuola, su valutazione dei responsabili di laboratorio e del dirigente scolastico, si assume il diritto di impedire l'accesso dell'operatore ad Internet per un certo periodo di tempo rapportato alla gravità commessa.

In caso di abuso, a seconda della gravità del medesimo, e fatte salve ulteriori conseguenze di natura penale, civile, amministrativa, pecuniaria (se trattasi di rottura, danni ai beni, …) potranno essere comminate le sanzioni disciplinari previste dalla normativa vigente.

Molta attenzione e cura deve essere posta in occasione di eventuali utilizzi di Social Network (Facebook, MySpace, ….). Ciò può avvenire solo se strettamente seguiti da docenti esperti in ciò. Comunque si suggerisce, prima dell'effettivo utilizzo di tali siti, di eseguire una sapiente ed attenta consultazione

dell'opuscolo "Social Network: attenzione agli effetti collaterali", visibile e scaricabile presso il sito dell'Autorità del Garante per la Privacy: www.garanteprivacy.it

I docenti che utilizzano il laboratorio di informatica sono tenuti ad illustrare didatticamente agli alunni i contenuti della Politica d'Uso Accettabile delle TIC tenendo conto ovviamente della loro età, evidenziando le opportunità e i rischi connessi all'uso della comunicazione tecnologica.

Più in particolare gli studenti saranno invitati a:

- Non inviare a nessuno la propria foto o quelle di altre persone;
- Non accedere mai a siti in cui viene chiesto un pagamento;
- Non comunicare a nessuno, **per nessuna ragione**, il numero di carta di credito o i dati bancari dei genitori o di conoscenti;
- Non fissare appuntamenti o incontri con persone conosciute attraverso la rete;
- Informare genitori e insegnanti nel caso fossero comparse informazioni o pagine che creano disagio o novità.

6) - Fornitore di servizi Internet

Il personale della scuola possiede già la propria casella di posta elettronica fornita dal Ministero della P.I. E' consentito, pertanto, l'utilizzo della posta elettronica personale per compiti connessi alla propria funzione.

Indirizzi di posta elettronica possono essere forniti solo a gruppi o a classi, ma mai a singoli studenti. Il traffico dei messaggi deve comunque essere controllato direttamente dal docente che assiste durante l'ora di laboratorio.

Si raccomanda tutto il personale docente che accompagna l'attività di laboratorio di avere grande cura per l'adozione di tutte le modalità di tutela dei dati personali, come indicato nel Disciplinare Interno adottato dalla scuola ed aggiornato annualmente.
Non è prevista la possibilità di creare account personali né di scaricare la propria posta sui computer della scuola. Inoltre:

- durante l'orario scolastico gli studenti, sempre guidati dall'insegnante, potranno utilizzare solo fornitori di servizi e-mail approvati dalla scuola e per soli scopi didattici e/o culturali;
- per la navigazione su Internet l'insegnante guiderà gli studenti alla ricerca di informazioni su piattaforme e motori di ricerca creati per la didattica:
    a) per le scuole dell'infanzia e primarie si suggeriscono i siti: www.educity.it – www.kidsfreeware.com/computer/surfing_browser.html – www.simpaticol.com – www.baol.it – www.bambini.it – www.girotondo.com –
- Si segnalano anche i suggerimenti e le informazioni messe a disposizione su Internet da organismi governativi quali www.italia.gov.it/chihapauradellarete/index.html www.poliziadistato.it/cittadino/consigli/internet.html - www.carabinieri.it/cittadino/CONSIGLI/tematici/internet.html
- gli alunni potranno inviare messaggi solo se tale procedura fa parte di un progetto di lavoro autorizzato dell'insegnante;

- gli alunni non devono rilevare dettagli o informazioni personali o di altre persone di loro conoscenza (indirizzi, numeri di telefono);
- l'invio e la ricezione di allegati non sono permessi e devono eventualmente essere concordati con l'insegnante;
- è vietato utilizzare catene telematiche di messaggi.

7) - Mailing list moderate, gruppi di discussione e chat room

Agli studenti non è consentito né l'accesso alle chat-room pubbliche e non moderate né l'utilizzo di telefoni cellulari durante l'orario scolastico.

Sarà consentito loro sia l'utilizzo dei gruppi di discussione messi a disposizione dalle piattaforme didattiche, sotto lo stretto controllo degli insegnanti, sia l'utilizzo di lettori iPod purché tali attività facciano parte di progetti di lavoro precedentemente autorizzati e concordati con l'insegnante responsabile.

La scuola, nella persona del Dirigente scolastico, riconoscendo la semplicità, la rapidità, l'economicità di questo servizio offerto da Internet, potrà utilizzare il sistema delle mailing list per comunicare con i docenti notizie di loro pertinenza. Occorrerà cautela nel momento in cui si dovessero trasferire notizie riguardanti dati personali: in questo caso sarebbe bene non riportare in bianco i nominativi di studenti.
Analogamente la scuola potrà utilizzare le mailing list per comunicare direttamente con gli alunni o con i loro genitori. L'uso della posta elettronica richiede cautele che diversificano rispetto quelle stabilite nella corrispondenza tradizionale. In primo luogo gli indirizzi di posta elettronica degli alunni e non devono essere divulgati. Questa cautela va applicata in modo molto attento sia se l'indirizzo è personale dell'alunno sia se l'alunno utilizza quello di un familiare. Nel caso di invii a gruppi di alunni o a gruppi compositi si devono evitare liste di indirizzi nei campi "To:" oppure "Cc:" in quanto questi campi sono visibili a tutti i destinatari, e così tutti gli indirizzi di posta possono essere acquisiti da tutti i destinatari del messaggio. E', pertanto, opportuno utilizzare il campo "Bcc:" così da restare nascosto ai destinatari del messaggio.

8) - Uso delle immagini e dei filmati nella scuola

La scuola usa documentare aspetti della vita scolastica anche mediante le immagini conservate attraverso fotografie o videoriprese di eventi riguardanti gite scolastiche, recite, foto di classe, uscite didattiche, recite teatrali, gare e premiazioni sportive ed altro ancora purché similari.

Tali immagini sono da considerare dati personali. Non vi è dubbio che in questi casi ricorra la funzione istituzionale; infatti la documentazione delle iniziative riproducenti momenti di vita scolastica corrisponde a finalità educativa, didattica e formativa.

Se le produzioni di fotografie o le effettuazioni di videoriprese dovessero essere effettuate direttamente dai genitori l'operazione esula dall'ambito di interesse del Codice sulla Privacy in quanto il trattamento è effettuato da persona fisica per fini esclusivamente personali: ciò è peraltro garantito dall'art. 5 comma 3. e puntualmente ribadito dal Garante in una Decisione del gennaio 2001.

Successivamente lo stesso Garante, in comunicati stampa, ha ribadito che le riprese video raccolte dai genitori, durante manifestazioni che riproducono momenti di vita scolastica, non violano la privacy in quanto niente hanno a che fare con la stessa: si tratta di immagini non destinate a diffusione, ma raccolte per fini personali o amicali e destinate ad un ambito familiare. Il loro uso è quindi del tutto legittimo. Verrà prestata particolare attenzione alla eventuale pubblicazione delle medesime immagini su Internet, e in particolare sui social network. In caso di comunicazione sistematica o diffusione sarà necessario ottenere il consenso delle persone presenti nelle fotografie e nei video.

Se la riproduzione fotografica è effettuata da un dipendente si riterrà lecita solo se lo stesso dipendente sarà destinatario di una designazione come incaricato che lo autorizza a ciò. Tutto il materiale fotografico ottenuto appartiene alla scuola in quanto realizzato nell'ambito del rapporto di lavoro anche con riferimento al connesso diritto alla riproduzione. La scuola, pertanto, vanta il diritto esclusivo sul materiale prodotto.

Se, infine, il fotografo è un professionista, la scuola verificherà le credenziali dello stesso e avrà cura di formalizzare il mandato con una lettera di incarico se il fotografo è un artigiano o con una lettera di responsabile se il fotografo è una società di servizi. La scuola farà in modo di mettere in contatto le famiglie con il fotografo così da prestare il loro consenso alla realizzazione fotografica in quanto il rilascio del consenso è necessario trattandosi del fatto che il fotografo è un soggetto privato.

La scuola adotterà la stessa procedura nel caso in cui la stessa gestisca eventi o manifestazioni, nel corso di un partenariato con soggetti esterni, le cui rappresentazioni fotografiche verranno usate per comunicare l'evento a mezzo stampa o televisione. In questo ultimo caso la scuola non formalizzerà con i soggetti preposti alla realizzazione fotografica alcuna lettera di incarico, però avrà cura di informare adeguatamente i genitori sull'uso che si vuole fare della ripresa e quindi consentire di esprimere il libero consenso al trattamento delle immagini.

Laddove è richiesto l'intervento del professionista esterno, gli interessati non potranno pretendere la restituzione del materiale fotografico secondo quanto fissato dalla legge sul diritto d'autore, Legge 633 del 22 aprile 1941. Di contro il fotografo deve garantire che si conformerà non soltanto alle prescrizione della suddetta legge sul diritto d'autore ma anche e soprattutto alle prescrizioni del Codice sulla *Privacy* non farcendo uso improprio delle immagini.

L'utilizzo di telefonini, di apparecchi per la registrazione di suoni e di immagini non è consentito. Può concedersi il loro utilizzo, alla presenza dei docenti, solo eccezionalmente per usi personali, e sempre nel rispetto dei diritti e delle libertà fondamentali delle persone coinvolte nonché della loro dignità con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali. Infine, sarà concesso registrare lezioni esclusivamente per scopi personali per motivi di studio individuale. Per ogni altro utilizzo ed eventuale diffusione, anche su Internet, è necessario preliminarmente informare adeguatamente le persone coinvolte nella registrazione (docenti, studenti,…) ed ottenerne il loro consenso scritto.

9) - Gestione del sito web della scuola

La commissione informatica gestisce le pagine del sito della scuola ed è sua responsabilità garantire che il contenuto pubblicato sia accurato e appropriato. Rientra nei compiti di detta commissiona informatica la revisione periodica dell'Informativa sul trattamento dei dati personali del sito della scuola**,** già pubblicata nello stesso.

La scuola detiene i diritti d'autore dei propri documenti che si trovano sul sito o di quei documenti per i quali è stato chiesto ed ottenuto il permesso dall'autore proprietario.

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

La scuola richiederà ai genitori attraverso un'autorizzazione con validità annuale, il permesso di pubblicare il materiale prodotto dagli alunni; inoltre le fotografie degli stessi non verranno pubblicate senza il consenso scritto dei loro genitori o tutori e il nome degli alunni non verrà allegato alle fotografie, ma sarà riportata soltanto la classe di frequenza.

Si provvederà a sfumare il volto degli alunni per i quali l'autorizzazione con è stata concessa, in modo da renderli non riconoscibili.

Le fotografie degli alunni della scuola verranno selezionate attentamente dagli insegnanti facenti parte della commissione informatica in modo tale che gruppi di alunni siano ritratti in attività didattiche a scopi documentativi.

Non sarà necessaria l'autorizzazione per l'inserimento di immagini fotografiche di adulti, qualora siano ritratti in un contesto generale. L'autorizzazione scritta verrà richiesta nel caso in cui si tratti di primi piani. Il sito web potrà, in sintesi, pubblicare tutto ciò che, nella prassi comune, può essere affisso sulle bacheche della scuola.
La scuola offre, all'interno del proprio sito web, tutta una serie di servizi alle famiglie ed ai fruitori esterni che rendono visibile l'attività della scuola.

Tutti i servizi offerti non potranno ricondursi, anche indirettamente, al trattamento di dati personali sensibili (ovvero quei dati personali idonei a rilevare l'origine etnica, le convinzioni religiose, filosofiche e d'altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a calettare religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rilevare lo stato di salute e la vita sessuale) o a dati giudiziari (ovvero i dati personali idonei a rivelare provvedimenti in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato).

10) - Informazioni sulla P.U.A. della scuola

Le regole di base relative all'accesso ad Internet verranno approvate dal Consiglio d'Istituto ed esposte nei laboratori di informatica.

Il Dirigente Scolastico ha il diritto di revocare l'accessibilità temporanea o permanente ai laboratori informatici a chi non si attiene alle regole stabilite.

Il personale scolastico avrà una copia della Politica d'Uso Accettabile della scuola, che dovrà essere sottoscritta e osservata scrupolosamente. Tutto il personale scolastico, pertanto, sarà coinvolto nel monitoraggio dell'utilizzo di Internet, nello sviluppo delle linee guida e nell'applicazione delle istruzioni sull'uso sicuro e responsabile di Internet.

Gli insegnanti firmeranno il documento che riporta le regole della Politica d'Uso Accettabile di Internet.
I genitori/tutori verranno informati della P.U.A. della scuola e potranno richiedere copia del presente regolamento.

Infine, la scuola, per consentire la massima diffusione del presente regolamento lo esporrà all'albo della sede e degli eventuali plessi, lo pubblicherà nel sito web della scuola e, a richiesta, potrà essere consultato presso la segreteria della stessa.

11) – Conclusioni

Le regole che sino tracciate segnalano al tempo stesso prospettive di ampliamento nell'uso delle ICT ed aspetti di criticità che richiedono attenzioni e cautele. Questi ultimi non devono prevalere sulle prime.

Le ICT non costituiscono soltanto uno strumento utile ed insostituibile, ma soprattutto il necessario sfondo operativo in cui il cittadino si colloca per esercitare i propri diritti , crescere culturalmente e affermarsi come oggetto nel rapporto con gli altri cittadini e con lo Stato. L'uso delle ICT a scuola da parte di tutti coloro che a vario titolo sono attori nel definirsi del rapporto educativo (studenti ed insegnanti, genitori, dirigenti, personale ausiliario, tecnico e amministrativo rientra in questo quadro come il primo necessario passo di una formazione destinata a non interrompersi dopo la adolescenza e a continuare per tutta la vita.
Proprio in ciò, nella dimensione formativa propria di tutte le attività che si svolgono a scuola, si risolve la problematicità del rapporto tra vantaggi che si conseguono attraverso l'uso delle ICT e cautele che è doveroso attuare. Il cittadino che poco prima dei sei anni entra nelle scuole primarie, imparerà a leggere, scrivere e far di conto – secondo una vecchia formula di recente molto rivalutata – imparerà anche a collocare fatti e oggetti nello spazio e nel tempo e, infine, imparerà anche a sviluppare un uso corretto e consapevole di strumenti di comunicazione di cui i suoi genitori, alla sua età, non potevano neppure avere nozione, semplicemente perché questi strumenti non esistevano ancora. Nella formazione di queste capacità, che sarà una di quelle caratterizzanti l'Europa della conoscenza delineata poco tempo fa nella Conferenza di Lisbona, la scuola non può non assumere un ruolo primario. Cautele ed attenzioni sono quelle necessarie in tutti i casi nei quali si affrontano con gli allievi le grandi questioni del rapporto con, e del rispetto verso, gli altri.

I percorsi formativi predisposti dal MIUR, i finanziamenti per le tecnologie che hanno consentito alle scuole di dotarsi di infrastrutture adeguate, il sempre maggiore uso che i docenti fanno delle ICT, tutto concorre a prefigurare uno scenario in cui le regole stabilite nel presente regolamento, potranno aiutare a sviluppare consapevolezza e a far conseguire risultati positivi a tutti i soggetti che nelle scuole si

accingeranno ad usare la tecnologia per la crescita culturale e civile degli allievi, di quei piccoli cittadini che nelle nostre aule diventano i cittadini protagonisti della società di domani.