Liceo Scientifico Statale “SANTI SAVARINO”
Con sezione Classica annessa - C.M. PAPS080008 - C.F.: 80018020828
Via Peppino Impastato, c/da Turrisi s.n.c. - 90047 PARTINICO (PA)
Tel. 0918780462 - Fax 0918780276
Plesso Liceo Linguistico via Palermo, 147 - Terrasini (Pa) Tel. 091/8684513
e-mail:paps080008@istruzione. it - PEC: paps080008@pec.istruzione.it

LICEO STATALE "S.SAVARINO" PARTINICO
Prot. 0003225 del 25/03/2021
06-11 (Uscita)

All’Albo on line
Al sito web
Amministrazione trasparente
Atti

REGOLAMENTO PER L’USO DELLE TECNOLOGIE INFORMATICHE E DELLA COMUNICAZIONE

Approvato con deliberazione del Consiglio d’Istituto n 37 del 12/02/2021

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

Premessa

Differenza tra Internet e web.

Spesso si parla di internet e di web come se fossero la stessa cosa. In realtà con è così.

Esiste una notevole differenza tra i due concetti. In breve.

La rete internet è l'infrastruttura tecnologica dove viaggiano i dati. Può essere immaginata come una specie di ferrovia digitale, con i propri binari (**canali**), stazioni (**server**) e regole (**protocolli**).

Il web è uno dei servizi internet che permette il trasferimento e la visualizzazione dei dati, sotto forma di ipertesto. Tutto ciò che vediamo sul nostro *browser.* Oltre al web esistono altri servizi come la posta elettronica, i *newgroups*, i trasferimenti FTP, ecc….

Un esempio chiarificatore. Quando si visualizza una pagina web sul *browser* si utilizza il web. Quando si scarica la posta elettronica sul computer, invece, non si utilizza il web. In entrambi i casi si usa la rete internet per trasferire i dati ma i **protocolli** sono diversi.

L'argomento è molto importante e la comprensione della notevole differenza si avverte conoscendo le date di nascita dei due concetti e la loro storica evoluzione. In breve si prova a fare una breve presentazione di Internet e, più in la, quella del web.

Internet e Web

In senso tecnico Internet è un network di computer-network: è infatti costituita da una serie di reti (private, pubbliche, aziendali, universitarie, commerciali) connesse tra loro fino a raggiungere una dimensione di accesso globale. Le reti sono interconnesse in senso fisico (wired e wireless) e in senso logico (distributed network); trasportano i dati e li indirizzano su una pluralità di dispositivi terminali (host, end system; dunque non solo computer in senso stretto) facendo ricorso a un medesimo gruppo di protocolli, l'Internet protocol suite. L'Internet protocol (IP) identifica i nodi della rete, mentre il trasporto viene generalmente gestito mediante uno standard di commutazione a pacchetto (packet switching).

I dati, tutti in formato digitale, comprendono le più svariate tipologie di informazioni, contenuti e servizi, come la posta elettronica (e-mail), le comunicazioni interpersonali in testo (chat) e in video, lo streaming audiovideo, lo scambio di file tra terminali (peer-to-peer) e, infine, le pagine e tutte le altre forme di documenti o repertori connesse tra di loro mediante rimandi ipertestuali (hyperlink) e forme di indirizzamento univoco (URL, Uniform resource locator) che compongono il servizio più conosciuto, il World Wide Web (noto anche come Web o W3).

Appare evidente che Internet e il Web non possono essere considerati sinonimi. Il Web è solo uno dei servizi supportati da Internet e dal punto di vista della configurazione del network complessivo rinvia al sottoinsieme di server che gestiscono documenti in formato HTML (Hypertext markup language), destinati a essere letti su terminali utente dai browser (Explorer, Netscape, Opera, Mozilla ecc.)

attraverso un protocollo dedicato al trasferimento dati in formato ipertestuale HTTP (Hypertext transfer protocol).
Il groviglio di termini tecnici, la complessità delle architetture, la pluralità di sistemi tecnologici e l'estrema differenziazione dei servizi descrive un universo in continua e accelerata trasformazione che sembra in grado di inglobare al suo interno tecnologie, sistemi mediali, forme culturali, stili di relazione sociale una volta rigorosamente segmentati e distinti. Ma questo universo complesso, storicamente prodotto per successive integrazioni e senza un'autorità centrale che ne orientasse in maniera univoca lo sviluppo, fonda le sue enormi potenzialità di ulteriore espansione su principî assolutamente semplici: l'univocità dei protocolli, la modularità della trasmissione dei dati per pacchetti, la struttura distribuita e ridondante del network. Questi principî non rappresentano solo componenti dell'ingegneria di sistema ma hanno ispirato e sono stati a loro volta piegati in forme del tutto impreviste dagli usi sociali, dando vita a un ecosistema composto da reti di macchine e reti di persone.

Internet dunque non è solo un'infrastruttura comunicativa veloce e affidabile ma anche un ambiente comunicativo e mediale, aperto e tendenzialmente paritario che non pone istituzionalmente vincoli di accesso. In virtù della sua architettura decentralizzata può assicurare connettività ubiqua in un contesto tecnologico flessibile e adattivo, senza fare riferimento ad alcun criterio gerarchico e ad alcuna necessità strutturale di controllo centralizzato. La metafora della rete, applicata sia a Internet sia al Web, il suo principale servizio, sottolinea:
(a) la possibilità per ogni nodo (inteso sia come computer o altro device terminale sia come utente) di essere sia emittente sia destinatario di comunicazioni;
(b) l'assenza di un unico centro, vale a dire di un unico autore, di un unico progetto, di una gerarchia prestabilita tra aree più o meno importanti del network.
L'architettura di molti servizi (a partire dai più noti, come il Web e la posta elettronica) prevede infatti una distinzione dei nodi della rete tra server e client, tra sistemi (hardware e software) che mettono a disposizione contenuti e servizi e altri che li utilizzano attraverso i loro terminali connessi alla rete. Il caso in cui diversi terminali dialoghino effettivamente tra pari (peer to peer), al di fuori della logica client-server, riguarda un numero ristretto di applicazioni, anche se genera volumi di traffico tra i nodi della rete sempre più rilevanti in conseguenza delle pratiche di file sharing: la condivisione e lo scambio di contenuti (musica, filmati, giochi ecc.) tra i terminali di singoli utenti, spesso aggirando le norme del diritto d'autore. La dimensione pubblica della rete Internet, in ogni caso, deriva non solo dalla condivisione di regole (protocolli) di comunicazione, ma anche dalla struttura di macchine server che rendono disponibili risorse e servizi per una molteplicità di terminali e per le esigenze differenziate degli utenti.

Il Web è un sistema di documenti in formato ipertestuale, posti in relazione per mezzo di link e accessibili mediante Internet. Per mezzo di un applicativo che prende il nome di web browser, istallato su una macchina client (non solo un personal computer ma anche uno schermo televisivo, un palmare, un telefono cellulare ecc.), l'utente può scaricare (download) dai web server e navigare (sfogliare) interattivamente attraverso link i repertori ipertestuali organizzati in pagine web, che contengono testo, immagini, video e altri formati multimediali (suoni, animazioni, immagini ecc.).
Nel corso degli anni Novanta in tutti i paesi del mondo si diffondono gli ISP (Internet service provider), organizzazioni commerciali che offrono a singoli utenti residenziali o a imprese l'accesso a Internet e alcuni servizi collaterali, come la gestione delle caselle personali di posta elettronica, la disponibilità di

spazio (hosting) per la pubblicazione on line di pagine web, la registrazione e la manutenzione di un dominio, cioè di un indirizzo univoco nel sistema URI (per es., http://www.comune.roma.it) che appartiene a un proprietario e costituisce un nodo di rete dove sono disponibili a vario titolo risorse e servizi di cui il titolare è (anche) legalmente responsabile. Le società di telecomunicazione, che esercitano il controllo sulle reti fisiche, svolgono normalmente la funzione di ISP di primo livello, anche perché assicurano la messa in opera e l'aggiornamento delle dorsali Internet. Gli utenti privati vengono allacciati direttamente da esse o da rivenditori del servizio di accesso al Web attraverso il modem, un dispositivo che rende possibile il traffico di dati tra sistemi informatici (web client/web server) per mezzo della normale rete telefonica, di altre tipologie di cavo o di radiofrequenza. Il caratteristico rumore del modem, che compone il numero di telefono dell'ISP e proietta il computer in rete, accompagna le esperienze dei pionieri che si affacciavano nel cyberspazio. Un termine, questo, coniato dall'autore canadese di fantascienza William F. Gibson, con cui si indica il nuovo ambiente virtuale.

Tutte le parti chiamate in causa nel presente documento devono leggerlo attentamente per accertarsi di averlo compreso in ogni sua parte e di recepirne i contenuti per applicarli con consapevolezza.

Il Liceo Santi Savarino elabora il presente Regolamento, periodicamente revisionabile, relativo alla Politica d'Uso Accettabile delle Tecnologie dell'Informazione e della Comunicazione. Lo scopo del presente documento è quello di garantire un uso corretto e responsabile delle apparecchiature informatiche in dotazione al Liceo 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 bullismo, il rispetto verso gli altri.
Il presente Regolamento, che definisce l'aspetto della Policy d'Istituto 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. Buone pressi di comportamento da seguire;
2. I vantaggi di internet a scuola;
3. Informazione per il personale scolastico, per gli studenti e per i genitori;
4. Oggetto ed ambito di applicazione;
5. Diritti e responsabilità;
6. Amministratore di Sistema;
7. Utilizzo del Personal computer;
8. Utilizzo della rete informatica;
9. Utilizzo di Internet;
10. Utilizzo della posta elettronica;
11. Utilizzo delle password;
12. Utilizzo dei supporti magnetici;
13. Utilizzo dei Pc portatili;
14. Utilizzo delle stampanti e del materiale di consumo;
15. Accertamento dei rischi e valutazione dei contenuti di internet;

16. Strategie della scuola per garantire la sicurezza delle TIC;
17. Cloud computing: indicazioni per un uso consapevole dei servizi;
18. Norme e linee guida;
19. Fornitore di servizi internet;
20. Uso delle immagini e dei filmati nella scuola
21. Gestione del sito web della scuola;
22. Informazioni sulla Politica d'Uso Accettabile della scuola;
23. Conclusioni.

Art. 1 - Buone prassi comportamentali da seguire

Tutti gli utenti che utilizzano internet devono rispettare:

1. La legislazione vigente in materia di comunicazione su internet applicata;
2. La netiquette: etica e norme di buon uso dei servizi di rete.

Art. 2 -I vantaggi di Internet a Scuola

Il curricolo scolastico prevede che gli studenti imparino a reperire materiale, recuperare documenti e scambiare informazioni attraverso l'uso delle TIC. Internet offre sia agli studenti sia al personale docente una vasta scelta di risorse e opportunità di scambi culturali con persone anche di altri paesi. Inoltre, su internet si possono recuperare risorse su tempo libero, attività scolastiche e sociali, proposte collaborativo–lavorative.

La scuola propone, sia agli studenti sia al personale docente, di utilizzare internet al fine di promuovere l'eccellenza in ambito didattico, attraverso la condivisione delle risorse, l'innovazione e la comunicazione.

Per gli studenti ed il personale docente l'accesso ad internet è un privilegio ed un diritto. L'accesso ad internet permette al personale docente di svolgere in modo agevole ed efficace diverse funzioni rilevanti da un punto di vista professionale, in primo luogo l'autoaggiornamento e la partecipazione ad iniziative di e-learning avviate dal Ministero. La possibilità di accedere da scuola alle risorse documentarie tramite internet diviene un fattore imprescindibile per lo svolgimento della professione e per un uso corretto ed efficace delle nuove tecnologie per la didattica.

L'accesso ad internet diventa per gli allievi uno strumento di acquisizione del sapere che si affianca agli strumenti tradizionali e lo rende implicitamente oggetto di particolare attenzione per la formazione dei giovani. L'approccio all'uso delle TIC si presenta quindi come ambito formativo non esclusivamente disciplinare ma trasversale rispetto all'azione educativa dell'istituto.

Esiste però la possibilità che gli studenti trovino materiale inadeguato ed illegale su internet; a tal proposito il Liceo deve prendere opportune precauzioni, limitando l'accesso a internet. Gli insegnanti hanno la responsabilità di guidare gli studenti nelle attività on line, di stabilire obiettivi chiari nell'uso di internet e di insegnarne un uso accettabile e responsabile. L'obiettivo principale resta quello di arricchire ed ampliare le attività didattiche, secondo quanto prevede il curricolo scolastico, l'età e la maturità degli studenti.

Per il personale ATA, oltre alle attività legate alle proprie mansioni (trasmissioni telematiche al ministero, monitoraggio progetti, utilizzo della piattaforma di segreteria, …), l'utilizzo di internet è consentito e promosso per tutte quelle attività legate all'aggiornamento e formazione del proprio profilo professionale.

Art. 3 – Informazione per il personale scolastico, per gli studenti e per i genitori

Il personale scolastico viene informato delle regole dell'acceso ad internet dell'istituto e sul sito web della scuola. Esso potrà richiedere una copia del documento; è inoltre consapevole che l'uso di internet verrà monitorato e segnalato e che tutto il personale scolastico sarà coinvolto nello sviluppo del regolamento di utilizzo della rete della scuola e nell'applicazione delle istruzioni sull'uso sicuro e responsabile di internet.
In caso di dubbi legati alla legittimità di una certa istanza utilizzata in internet, l'insegnante dovrà contattare il Dirigente scolastico o il responsabile della gestione delle TIC per evitare malintesi. Gli insegnanti saranno inoltre provvisti di informazioni concernenti le problematiche sul diritto d'autore che vengono applicate anche alla scuola.

Le regole di base relative all'accesso ad internet descritte nel presente documento saranno esposte nei laboratori di informatica, insieme al regolamento sull'uso delle TIC, e pubblicate sul sito della scuola.
Gli studenti saranno informati che l'utilizzo di internet è monitorato e verranno loro date le istruzioni per un uso responsabile e sicuro di internet.
Gli studenti e i loro genitori devono prendere visione del presente documento.

I genitori vengono informati delle regole dell'uso internet dell'istituto e sul sito web della scuola. Essi potranno richiedere una copia del documento; è auspicabile che le regole sull'uso accettabile e responsabile di internet all'interno dell'istituto siano condivise e conseguite dalle famiglie anche nell'ambiente domestico.
Eventuali commenti o suggerimenti connessi possono essere inviati all'attenzione del Dirigente Scolastico.

Art. 4 - Oggetto e ambito di applicazione

Il presente regolamento e le sue premesse che ne sono parte integrante, disciplinano le modalità di accesso, di uso delle risorse informatiche dell'Istituto (rete, apparecchiature e risorse infrastrutturali, patrimonio informativo e software).
Le risorse infrastrutturali sono le componenti hardware/software e gli apparati elettronici collegati alla rete informatica della scuola. Il patrimonio informativo è l'insieme delle banche dati in formato digitale e in generale tutti i documenti prodotti tramite l'utilizzo dei suddetti apparati. Le risorse software sono i sistemi operativi e i programmi acquisiti legalmente dall'Istituto).
Il presente regolamento si applica a tutti gli utenti interni che sono autorizzati ad accedere alla rete della scuola: impiegati amministrativi, tecnici, docenti, collaboratori scolastici ed alunni. Si applica anche a taluni utenti esterni, quali i collaboratori esterni, ditte fornitrici di software che effettuano attività di manutenzione limitatamente alle applicazioni di loro competenza, ditte fornitrici di hardware o delegate alla sua manutenzione (è consentita la visualizzazione di files solo per quanto strettamente indispensabile), eventuali enti esterni autorizzati da apposite convenzioni all'accesso a specifiche banche dati con le modalità stabilite dalle stesse.

Art. 5 - Principi generali – Diritti e Responsabilità

Ogni utente è responsabile civilmente e penalmente del corretto uso delle risorse informatiche, dei servizi/programmi ai quali ha accesso e dei propri dati. Tutti i soggetti interagenti, a qualunque titolo, col sistema informatico dell'Istituto sono anche responsabili di eventuali danni erariali conseguenti.

Per motivi di sicurezza e protezione dei dati, ogni attività compiuta nella rete informatica è sottoposta a registrazione in files-registro; la registrazione riguarda orario di inizio e fine dell'accesso al sistema e all'account che ha operato. Detti files possono essere soggetti a trattamento solo per fini istituzionali, per attività di monitoraggio e controllo; possono essere messi a disposizione dell'autorità giudiziaria in caso di accertata violazione di normativa vigente. La riservatezza delle informazioni in essi contenute è soggetta a quanto dettato dal regolamento europeo 679/2016 e normativa collegata.
L'Istituto, per fini legati alla sicurezza dell'intero sistema informativo, dispone di strumenti per il monitoraggio e il controllo della navigazione in internet.

Art. 6 - Amministratore di Sistema

Gli Amministratori di Sistema sono i soggetti cui è conferito il compito di sovrintendere alle risorse informatiche dell'Istituto e a cui sono consentite le seguenti attività:

1. Gestire l'hardware e il software di tutte le strutture tecniche informatiche di appartenenza dell'Istituto, collegate in rete o meno;
2. Gestire esecutivamente (creazione, attivazione, disattivazione e tutte le relative attività amministrative) gli account di rete e i relativi privilegi di accesso alle risorse, assegnati agli utenti della Rete Informatica istituzionale, secondo le direttive impartite dal Titolare;
3. Utilizzare le credenziali conservate dal "Custode delle password" oppure le credenziali di accesso di amministrazione del sistema o l'account di un utente tramite reinizializzazione della relativa password, per accedere ai dati o alle applicazioni presenti su una risorsa informatica assegnata ad un utente in caso di prolungata assenza, irrintracciabilità o impedimento dello stesso. Tale utilizzo deve essere esplicitamente richiesto dal Titolare per l'utente assente o impedito, e deve essere limitato al tempo strettamente necessario al compimento delle attività indifferibili per cui è stato richiesto.
4. Solo se rientranti nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori, eseguire le seguenti attività:
    a. Monitorare o utilizzare qualunque tipo di sistema informatico o elettronico per controllare il corretto utilizzo delle risorse di rete, dei computer e degli applicativi;
    b. Creare, modificare, rimuovere o utilizzare qualunque account o privilegio, attesa l'autorizzazione del Titolare;
    c. Rimuovere programmi software dalle risorse informatiche assegnate agli utenti;
    d. Rimuovere componenti hardware dalle risorse informatiche assegnate agli utenti.

Art. 7- Utilizzo dei personal computer

Il personal computer affidato al dipendente è uno strumento di lavoro. Ogni utilizzo non inerente all'attività professionale può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Pertanto:

a) L'uso dell'elaboratore con profilo di accesso specifico (utenti dell'area Amministrativa e di Sistema, Sistema integrato del registro elettronico, piattaforma di e-learning, account individuali riservati) deve essere protetto da password e non divulgata. Gli account destinati al trattamento di dati amministrativi e sensibili sono custoditi a cura del Titolare del trattamento dati.

b) I preposti all'amministrazione del sistema, nell'espletamento delle funzioni legate alla sicurezza e alla manutenzione informatica, avranno la facoltà di accedere in qualunque momento anche da remoto a tutte le postazioni e a tutti gli account.
c) Il personal computer deve essere spento al termine dell'orario delle lezioni o di servizio, comunque prima di lasciare gli uffici, i laboratori di informatica, le aule. Lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso. Al termine di qualunque sessione riservata di lavoro o di assenza temporanea è obbligatorio uscire dall'account o bloccare il computer.
d) L'accesso ai dati presenti nel personal computer di area amministrativa potrà avvenire quando si rende indispensabile ed indifferibile l'intervento, ad esempio in caso di prolungata assenza od impedimento dell'incaricato, informando tempestivamente l'incaricato dell'intervento di accesso realizzato.
e) É vietato installare autonomamente programmi informatici sui server salvo autorizzazione esplicita dell'amministratore di sistema, e sui PC salvo autorizzazione del Titolare, in quanto sussiste il grave pericolo di portare virus informatici o di alterare la stabilità delle applicazioni dell'elaboratore. L'inosservanza di questa disposizione, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre la struttura a gravi responsabilità civili ed anche penali in caso di violazione della normativa a tutela dei diritti d'autore sul software (D. Lgs. 518/92 sulla tutela giuridica del software e l. 248/2000 nuove norme di tutela del diritto d'autore) che impone la presenza nel sistema di software regolarmente licenziato o comunque libero e quindi non protetto dal diritto d'autore.
f) É vietato modificare le caratteristiche impostate sul proprio PC, salvo con autorizzazione esplicita degli amministratori di sistema o del Titolare.
g) É vietato inserire password locali alle risorse informatiche assegnate (come ad esempio password che non rendano accessibile il computer agli amministratori di rete), se non espressamente autorizzati e dovutamente comunicate agli amministratori di sistema;
h) É vietata l'installazione sul proprio PC di dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, dischi esterni, i-pod, telefoni, ecc.), se non con l'autorizzazione espressa dell'amministratore di sistema o del Titolare. Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente l'amministratore di sistema o Titolare nel caso in cui vengano rilevati virus o eventuali malfunzionamenti.

Art. 8 - Utilizzo della rete informatica

Le unità di rete sono aree di condivisione di informazioni strettamente professionali sulle quali vengono svolte regolari attività di controllo, amministrazione e backup e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia legato all'attività lavorativa non può essere dislocato in queste unità.

In presenza di reti locali con dominio, i files relativi alla produttività individuale possono essere salvati sul server e i limiti di accesso sono regolarizzati da apposite procedure di sicurezza che suddividono gli accessi tra gruppi e utenti aventi profili di autorizzazione diversi.

L'amministratore di sistema può, in qualunque momento, procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza o in violazione del presente regolamento sia sui PC degli autorizzati sia sulle unità di rete.
Le password d'ingresso alla rete ed ai programmi sono segrete e non vanno comunicate a terzi.
Costituisce buona regola la periodica **pulizia degli archivi**, con cancellazione dei files obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati: è infatti assolutamente da evitare un'archiviazione ridondante.
E' importante togliere tutte le condivisioni dei dischi o di altri supporti configurate nel PC se non strettamente necessarie (e per breve tempo) allo scambio dei file con altri colleghi. Esse sono infatti un ottimo "aiuto" per i software che cercano di minare la sicurezza dell'intero sistema.
É compito degli amministratori di sistema provvedere alla creazione e alla manutenzione di aree condivise sul server per lo scambio dei dati tra i vari utenti.
Nell'utilizzo della rete informatica è fatto divieto di:

1. Utilizzare la Rete in modo difforme da quanto previsto dal presente regolamento;
2. Agire deliberatamente con attività che influenzino negativamente la regolare operatività della Rete e ne restringano l'utilizzabilità e le prestazioni per altri utenti
3. Effettuare trasferimenti non autorizzati di informazioni (software, dati, ecc);
4. Installare componenti hardware non compatibili con l'attività istituzionale;
5. Rimuovere, danneggiare o asportare componenti hardware;
6. Utilizzare qualunque tipo di sistema informatico o elettronico per controllare le attività di altri utenti, per leggere, copiare o cancellare file e software di altri utenti
7. Utilizzare software visualizzatori di pacchetti TCP/IP (sniffer), software di intercettazione di tastiera (keygrabber o keylogger), software di decodifica password (cracker) e già in generale software rivolti alla violazione della sicurezza del sistema e della privacy;
8. Usare l'anonimato o servirsi di risorse che consentano di restare anonimi.

Art. 9 - Utilizzo di internet

I PC abilitati alla navigazione in Internet costituiscono uno strumento necessario e prezioso per lo svolgimento dell'attività professionale.
Nell'uso di internet e della posta elettronica non sono consentite le seguenti attività:

1. L'uso di internet per motivi personali (ad esempio facebook).
2. L'accesso a siti inappropriati (esempio siti pornografici, di intrattenimento, ecc.);
3. Lo scaricamento (download) di software e di file non necessari all'attività istituzionale, sia perché potrebbero celare minacce al buon funzionamento del sistema, sia perché software privi di licenza comportano gravissime sanzioni economiche e penali per il Datore di lavoro ed eventualmente anche per il dipendente;
4. Utilizzare programmi per la condivisione e lo scambio di file in modalità peer to peer (Napster, Emule, Winmx, e-Donkey, ecc.);
5. Accedere a flussi in streaming audio/video da Internet per scopi non istituzionali;
6. Un uso che possa in qualche modo recare qualsiasi danno all'Istituto o a terzi.

Il dipendente non deve eseguire download di files eseguibili o documenti da siti Web, HTTP o FTP non conosciuti. Si ricorda che la frequentazione di siti non conosciuti o lo scaricamento di files da fonti non garantite possono introdurre virus o altro malware, che possono creare inconvenienti

gravissimi, con perdita di dati, blocco operativo e danni economici importanti. L'imprudente autore può essere chiamato a risponderne in via disciplinare e per il danno recato.

Art. 10 - Utilizzo della posta elettronica

La casella di posta assegnata dall'Istituto, è uno strumento di lavoro e le persone assegnatarie delle caselle di posta elettronica sono responsabili del loro corretto utilizzo.

É fatto divieto di utilizzare le caselle di posta elettronica della struttura per la partecipazione a dibattiti, forum o mailing-list, salvo diversa ed esplicita autorizzazione, che esulino dagli scopi della scuola.

É buona norma evitare messaggi completamente estranei al rapporto di lavoro o alle relazioni tra colleghi. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.

Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali con l'istituto ricevuta da personale non autorizzato, deve essere visionata ed inoltrata al Direttore amministrativo, o in ogni caso è opportuno fare riferimento alle procedure in essere per la corrispondenza ordinaria.

La documentazione elettronica che viene contraddistinta da diciture od avvertenze dirette ad evidenziarne il carattere riservato o segreto, non può essere comunicata all'esterno senza preventiva autorizzazione del Responsabile del trattamento.

Per la trasmissione di files all'interno della struttura è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati (ad esempio per dimensioni superiori a 25 MB è preferibile utilizzare le cartelle di rete condivise).

E' obbligatorio controllare i file attachments (allegati) di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web, HTTP o FTP non conosciuti) e accertarsi dell'identità del mittente.

In particolare, nell'uso della posta elettronica non sono consentite le seguenti attività:

1. La trasmissione a mezzo di posta elettronica di dati articolari, confidenziali e personali di alcun genere, salvo i casi espressamente previsti dalla normativa vigente in materia di protezione dei dati personali (d. lgs. 196 del 30/6/2003 come modificato dal decreto legislativo 101 del 2018) e inerenti le ragioni di servizio;
2. L'apertura di allegati ai messaggi di posta elettronica senza il previo accertamento dell'identità del mittente;
3. Inviare tramite posta elettronica informazioni quali user-id, password, configurazioni della rete interna, indirizzi e nomi dei sistemi informatici.

Art. 11 - Utilizzo delle password

Le password di ingresso alla rete, di accesso ai programmi e dello screensaver, sono previste ed attribuite dai referenti di sistema, ovvero dal Titolare del trattamento dei dati.

E' necessario procedere alla modifica della password almeno ogni sei mesi, con contestuale verbalizzazione dell'operazione nell'apposito registro gestito dal Dirigente scolastico.

Le password possono essere formate da lettere (maiuscole o minuscole) e numeri utilizzando almeno 1 carattere speciale, ricordando che lettere maiuscole e minuscole hanno significati diversi per il sistema; devono essere composte da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'autorizzato.

Nel caso si sospetti che la password abbia perso la segretezza, deve essere immediatamente sostituita, dandone comunicazione scritta all'Incaricato della custodia delle password.
Qualora l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia, per iscritto, al Titolare.

Art. 12 -Utilizzo dei supporti magnetici

Tutti i supporti magnetici riutilizzabili (chiavi USB, CD e DVD) contenenti dati particolari (art. 9 e 10 del Regolamento europeo) devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato. Una persona esperta potrebbe infatti recuperare i dati memorizzati anche dopo la loro cancellazione.
I supporti magnetici contenenti dati particolari devono essere custoditi in archivi chiusi a chiave.
Tutti i supporti magnetici riutilizzabili (chiavi USB, CD riscrivibili e DVD) obsoleti devono essere consegnati all'Amministratore di Sistema per l'opportuna distruzione.
Ogni qualvolta si procederà alla dismissione di un Personal Computer l'Amministratore di Sistema provvederà alla distruzione o all'archiviazione protetta delle unità di memoria interne alla macchina stessa (hard-disk, memorie allo stato solido).

Art. 13 - Utilizzo di PC portatili

L'utente è responsabile del PC portatile assegnatogli e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.
Ai PC portatili si applicano le regole di utilizzo previste per i PC connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.
I PC portatili utilizzati all'esterno (convegni, lavoro domestico autorizzato, ecc…), in caso di allontanamento devono essere custoditi in un luogo protetto.

Art. 14 - Utilizzo delle stampanti e dei materiali di consumo

L'utilizzo delle stampanti e dei materiali di consumo in genere (carta, inchiostro, toner, supporti digitali come CD e DVD) è riservato esclusivamente ai compiti di natura strettamente istituzionale.
Devono essere evitati in ogni modo sprechi dei suddetti materiali o utilizzi eccessivi.
É cura dell'utente effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni. É buona regola evitare di stampare documenti o file non-adatti (molto lunghi o non- supportati, come ad esempio files di contenuto grafico) su stampanti comuni. In caso di necessità la stampa in corso può essere cancellata.

Art. 15 - 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 17 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* (minimo 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 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 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, bullismo ed ancora altri eventi) e, qualora ne venissero a contatto, devono riferire immediatamente il fatto all'insegnante o al docente responsabile del laboratorio.

Art. 16 - Strategie della scuola per garantire la sicurezza delle TIC

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 le seguenti e valgono per tutti gli utenti stabili od occasionali:

- 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, asportare deliberatamente programmi software per scopi personali o per altri motivi non pertinenti alle attività didattiche;
- E' assolutamente vietato installare autonomamente programmi informatici sui server (salvo autorizzazione espressa dell'amministratore di sistema) e sui PC (salvo autorizzazione del titolare), in quanto sussiste il grave pericolo di importare virus informatici o di alterare la stabilità delle applicazioni dell'elaboratore. L'inosservanza di questa disposizione, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre la struttura a gravi responsabilità civili ed anche penali in caso di violazione della normativa a tutela dei diritti d'autore sul software (d. lgs. 518/1992 sulla tutela giuridica del software e l. 248/2000 sulle norme di tutela del diritto d'autore) che impongono la presenza nel sistema di software regolarmente licenziati o comunque libero e quindi non protetto dal diritto d'autore;
- 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;
- E' fatto divieto di utilizzare software antivirus non aggiornato costantemente e non licenziato e quindi non protetto dal diritto d'autore;
- L'utilizzo di CD personali e/o di chiavette è consentito previa autorizzazione di un docente facente parte della commissione informatica, che li sottopone preliminarmente 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, …..
- E' vietata l'installazione sul proprio PC di dispositivi di memorizzazione, comunicazione o altro (masterizzazioni, dischi esterni, ..) se non con l'autorizzazione espressa dell'amministratore di sistema o del titolare. Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo subito l'amministratore di sistema o il titolare nel caso in cui vengano rilevati virus o eventuali malfunzionamenti.

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

Art. 17 – 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 tutte 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.

In 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 prassi 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 esercitabile 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 elaborativa)
- 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 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

Art. 18 - 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.

Art. 19 - 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. Il Liceo Santi Savarino ha creato per tutto il personale scolastico, il Presidente del CdI e gli alunni account personali edu.

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.
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:
- 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.

Art. 20 - 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 facendo 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.

Art. 21 - Gestione del sito web della scuola

La FS **Gestione sito web e multimedialità** gestisce le pagine del sito della scuola ed è sua responsabilità garantire che il contenuto pubblicato sia accurato e appropriato. Rientra nei suoi compiti 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 carattere 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).

Art. 22 - 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.

Art. 23 – Osservanza delle disposizioni in materia di Privacy

E' fatto obbligo attenersi scrupolosamente a tutte le disposizioni in materia di Privacy prescritte dal Regolamento europeo 679/2016 e dal decreto legislativo 196 del 2003 così come modificato da decreto legislativo 101 del 2018.
Gli strumenti tecnologici considerati costituiscono tutti strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa, anche ai sensi e per gli effetti dell'art. 4 comma 2 della l. 300/1970; conseguentemente, le informazioni raccolte sulla base di quanto indicato nel presente regolamento possono essere utilizzati a tutti i fini connessi al rapporto di lavoro, essendone stata data informazione ai lavoratori, sulle modalità di uso degli strumenti stessi, sugli interventi che potranno venire compiuti nel sistema informatico della scuola.

Art. 24 – Conclusioni

Le regole che sono 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 fare i conti – 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.

Il Presidente del C.d.I

Avv Passannanti Antonio

Il Dirigente Scolastico

Prof.ssa Vincenza Vallone