

ISTITUTO TECNICO ECONOMICO PIETRO MARTINI
DISCIPLINARE INTERNO PER L'USO DI INTERNET E
DELLA POSTA ELETTRONICA



30/08/17

Delibera del Consiglio di Istituto del 30/08/2017

ISTITUTO TECNICO ECONOMICO PIETRO MARTINI DISCIPLINARE INTERNO PER L'USO DI INTERNET E DELLA POSTA ELETTRONICA

IL CONSIGLIO DI ISTITUTO

VISTA	la L. n. 241 del 07/08/1990 e ss. ii. mm.;
VISTO	il D. Lgs. 19/03/96 <i>Modifiche e integrazioni al D. Lgs. N. 626/1994 controlli operati tramite sistemi aziendali</i> ;
VISTO	il DPR del 28/12/2000 n. 445 <i>Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa</i> ;
VISTO	il D. Lgs. n. 196 del 30/06/2003 <i>Codice in materia di protezione di dati personali</i> ;
VISTO	il D.M. n. 305 del 07/12/2006, n. 305 <i>Regolamento recante identificazione dei dati sensibili e giudiziari</i> ;
VISTO	il D. Lgs. n. 82 del 07/03/2005 <i>Codice dell'Amministrazione Digitale e ss. ii. (CAD)</i> ;
VISTA	la Direttiva del Consiglio dei Ministri n. 2/2009 del 26/05/2009 <i>Utilizzo di Internet e della casella di posta elettronica istituzionale sul luogo di lavoro</i> ;
VISTA	la Direttiva del Presidente del Consiglio dei Ministri del 1 agosto 2015 <i>Misure minime di sicurezza ITC per le Pubbliche Amministrazioni</i> , pubblicata in GU con circolare AgID n. 2 del 18 aprile 2017.
CONSIDERATO	che l'Istituto tra i vari strumenti di lavoro, ha messo a disposizione dei dipendenti accessi ad internet e servizi di caselle di posta elettronica per l'intero svolgimento delle mansioni e compiti loro affidati;
RICHIAMATO	il principio generale, in applicazione di quanto disposto dagli Artt. 2104 e 2105 C.C. che l'utilizzo delle risorse ITC che la scuola mette a disposizione dei dipendenti deve sempre ispirarsi a criteri di diligenza, fedeltà e correttezza normalmente adottati nell'ambito dei rapporti di lavoro, in modo che siano adottate tutte le cautele e le precauzioni necessarie per evitare le possibili conseguenze dannose che un utilizzo non avveduto degli strumenti in questione può provocare;
VISTO	il DPR 16 aprile 2013, n. 62 <i>Regolamento recante codice di comportamento dei dipendenti pubblici, a norma dell'articolo 54 del decreto legislativo 30 marzo 2001, n. 165</i> , e in particolare l'Art 11, comma 3, che stabilisce che il dipendente utilizza il materiale o le attrezzature di cui dispone per ragioni di ufficio e i servizi telematici e telefonici dell'ufficio nel rispetto dei vincoli posti dall'amministrazione;
RILEVATO	che l'Autorità Garante per la Privacy ha inteso precisare che è opportuno, da parte dei Datori di Lavoro, adottare un disciplinare interno redatto in modo chiaro, senza formule generiche ed adeguatamente pubblicizzato;
RITENUTO	pertanto, di dover adottare apposito regolamento per l'utilizzo di Internet e della Posta Elettronica, nel quale regolamento è tra l'altro precisato che gli stessi sono strumenti aziendali e come tali soggetti anche a controlli secondo i principi ed i criteri di cui ai paragrafi 5, 6 e 7 del citato Provvedimento del Garante e della normativa in tema di Protezione dei dati personali (D. Lgs. 196/2003 n. 196) e del D.M. 05 del 7 dicembre 2006

TENUTO CONTO	che il Regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori, interni o esterni, della scuola, agli esperti esterni, ai collaboratori a progetto ed a quelli durante il periodo di stage a prescindere dal rapporto contrattuale con la stessa intrattenuto;
VISTE	le Linee guida del Garante per posta elettronica e internet, pubblicate in GU n. 58 del 10/03/2007;

EMANA

il seguente **Disciplinare Interno per l'uso di Internet e della posta elettronica** al fine di descrivere caratteristiche e regole di utilizzo della rete Internet e della Posta elettronica e di informare tutti i lavoratori sui controlli effettuati sul trattamento dei dati da loro elaborati.

Articolo I - PREMESSA

L'uso degli strumenti informatici, della posta elettronica e l'accesso ad Internet da parte delle amministrazioni pubbliche si va sempre più diffondendo sotto l'impulso della nuova legislazione, con l'obiettivo di migliorare l'efficienza operativa, contenere i costi ed assicurare una maggiore qualità delle prestazioni.

I servizi informativi sono ormai diventati fondamentali anche per gli istituti scolastici che sempre più devono utilizzare strumenti come la posta elettronica ed Internet per fornire servizi all'utenza e per migliorare la propria efficienza nell'ottica di una sempre più estesa dematerializzazione. La rete Internet è una risorsa strategica per arricchire ed integrare gradualmente le modalità comunicative della didattica tradizionale e per creare nuovi contesti di apprendimento, oltre che per rispondere alle esigenze di efficienza ed efficacia dei processi gestionali e amministrativi.

Ciò rende ancora più necessario adottare adeguate ed opportune misure di sicurezza volte a proteggere la disponibilità e l'integrità delle risorse informative e a tutelare la riservatezza dei dati personali di tutti. A questo proposito si richiama quanto viene riportato anche dalle Linee Guida per la Sicurezza ICT delle Pubbliche Amministrazioni del già CNIPA, attualmente AgID (Agenzia per l'Italia Digitale della Presidenza del Consiglio dei Ministri):

"Tutti i dipendenti dell'Amministrazione sono tenuti ad utilizzare i servizi di rete solo nell'ambito delle proprie mansioni di lavoro, secondo direttive circostanziate, essendo consapevoli che ogni accesso ad Internet può essere facilmente ricondotto alla persona che lo ha effettuato. Occorre quindi che i dipendenti si comportino con il massimo livello di professionalità quando operano in Internet, evitando eventi dannosi, anche al fine di non danneggiare l'immagine dell'Amministrazione".

Dall'esame di diversi reclami, segnalazioni e quesiti pervenuti, il Garante per la protezione dei dati personali ha preso atto dell'esigenza di prescrivere ai datori di lavoro pubblici e privati alcune misure, necessarie o opportune, per conformare alle vigenti disposizioni in materia di *Privacy* il trattamento di dati personali effettuato per verificare il corretto utilizzo, nel rapporto di lavoro, della Posta elettronica e di Internet.

A tale scopo è stato emanato il provvedimento generale pubblicato sul Bollettino n. 81 del Marzo 2007 (<http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1387522>) e, successivamente, sulla Gazzetta Ufficiale – Serie generale n. 58 del 10.03.2007 (di seguito "il Provvedimento").

Con il presente disciplinare il Dirigente Scolastico dell'Istituto Tecnico Economico "Pietro Martini" di Cagliari (d'ora in poi *Istituto*), in quanto responsabile dell'erogazione dei servizi in oggetto nonché titolare del trattamento dati, fornisce concreto riscontro alle prescrizioni del Garante e si conforma a quanto previsto nelle conclusioni del Provvedimento, punto 2), lett. a).

Articolo II - PRINCIPI

Il presente disciplinare viene predisposto nel rispetto della vigente disciplina in materia di *Privacy*, con riguardo, in particolare, alle norme del D.Lgs. 196/03 (Codice in materia di protezione dei dati personali) che disciplinano il trattamento effettuato dai soggetti pubblici.

L'Istituto garantisce che il trattamento dei dati personali dei dipendenti, effettuato per verificare il corretto utilizzo della Posta elettronica e di Internet, si conforma ai seguenti principi:

- il principio di **necessità**, secondo cui i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite (art. 3 del Codice; par. 5.2 del Provvedimento);
- il principio di **correttezza**, secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori (art. 11, c. 1, lett. a), del Codice) poiché le tecnologie dell'informazione, in modo più marcato rispetto ad apparecchiature tradizionali, permettono di svolgere trattamenti ulteriori rispetto a quelli connessi ordinariamente all'attività lavorativa, anche all'insaputa o, comunque, senza la piena consapevolezza dei lavoratori (par. 3 del Provvedimento);
- principio di **pertinenza e non eccedenza** (par. 6 del Provvedimento), in virtù del quale:
 - i trattamenti devono essere effettuati per finalità determinate, esplicite e legittime (art. 11, c. 1, lett. b) del Codice; par. 4 e 5 del Provvedimento);
 - il datore di lavoro deve trattare i dati "nella misura meno invasiva possibile";
 - le attività di monitoraggio devono essere svolte solo da soggetti preposti (par. 8 del Provvedimento) ed essere "mirate sull'area di rischio, tenendo conto della normativa sulla protezione dei dati e, se pertinente, del principio di segretezza della corrispondenza" (Parere n. 8/2001, punti 5 e 12).

Articolo III – INFORMATIVA SULLE MODALITÀ DI UTILIZZO DELLA POSTA ELETTRONICA, INTERNET E INTRANET SUL DOMINIO ISTRUZIONE.IT

I servizi di posta elettronica del dominio *istruzione.it*, quelli forniti dal sito www.miur.gov.it e dalla intranet ministeriale sono direttamente gestiti dalla **Direzione Generale per i Sistemi Informativi** che ha diffuso specifiche informative in merito alle modalità di utilizzo dei suddetti servizi e a cui si rimanda integralmente per i servizi di posta elettronica @istruzione.it e @pec.istruzione.it, e dei servizi Intranet del MIUR.

Articolo IV – UTENTI AUTORIZZATI ALL'USO DI INTERNET

Per quanto riguarda l'uso delle dotazioni informatiche e l'accesso ad internet si individuano 4 tipologie di utenti:

- **Personale tecnico:** autorizzato all'uso limitatamente allo svolgimento delle proprie mansioni o alle disposizioni ricevute.
- **Personale amministrativo:** autorizzato all'uso per lo svolgimento dell'attività amministrativa.
- **Personale docente:** autorizzato all'uso per qualunque attività educativa, didattica e formativa.
- **Alunni:** autorizzato limitatamente all'attività educativa, didattica e formativa programmata dai docenti.

L'utilizzo dei servizi di accesso ad internet cessa o viene sospesa d'ufficio quando:

- non sussiste più la condizione di dipendente/studente o l'autorizzazione al loro uso;
- vi è il sospetto di manomissione dell'hardware o del software;
- in caso di diffusione o comunicazione a terzi da parte del dipendente di password, codici di accesso ecc.;
- in caso di accesso doloso a file o servizi non rientranti tra quelli autorizzati;
- ogni qual volta sussistano ragionevoli evidenze di una violazione degli obblighi dell'utente che mette a rischio il sistema.

Articolo V – MISURE DI TIPO ORGANIZZATIVO

1 Ubicazione postazioni di lavoro

Per quanto riguarda il personale amministrativo, ogni dipendente riceve indicazione della postazione di lavoro a lui assegnata al momento della presa di servizio, ovvero in caso di cambiamento della propria posizione. L'uso di tale postazione non è tuttavia da ritenersi esclusivo e ciascun dipendente a seconda delle necessità potrà operare su altro PC non direttamente assegnato ***usando sempre la propria credenziale di accesso personale*** (nome utente e password).

L'accesso ad Internet da parte del personale tecnico, docente e degli alunni potrà avvenire nelle classi, nei laboratori ed in qualunque altro luogo a tale attività destinato.

2 Sistema di autenticazione

Accesso alle macchine di segreteria

Al fine di ridurre al minimo il rischio di impieghi abusivi, l'accesso alle postazioni destinate all'attività amministrativa è protetto tramite sistema di autenticazione che richiede l'immissione di un apposito codice utente e della relativa password. La gestione degli utenti è fatta in maniera centralizzata sul server di segreteria e nel quale potranno quindi essere conservate informazioni relative agli accessi dei singoli utenti.

Accesso ai PC delle LIM

L'accesso ai PC delle postazioni LIM collocate nelle aule è protetto tramite sistema di autenticazione che richiede l'immissione di un apposito codice utente e della relativa password. La gestione degli utenti è affidata ad un server destinato alla gestione dell'attività didattica e distinto dal server della segreteria. Le credenziali di accesso al dominio della didattica che consentono l'accesso alle postazioni LIM verranno fornite a tutti i docenti.

Accesso ai PC dei Laboratori

Tutti i laboratori sono destinati all'attività didattica ordinaria con le classi o straordinaria per progetti specifici e autorizzati e che, per via della disciplina insegnata, non possono fare a meno di utilizzare il mezzo informatico. Di norma, le discipline che saranno inserite di diritto nell'orario dei laboratori di Informatica e di Lingue sono: Informatica, Lingue Straniere, Economia Aziendale. Tutte le altre discipline possono trovare posto negli stessi laboratori, inserendosi nelle ore che restano libere rispetto a quelle su menzionate. Per poter utilizzare i laboratori, i docenti devono farne richiesta al direttore di laboratorio e all'assistente tecnico col quale concorderanno l'orario settimanale di loro interesse. Nei laboratori occorre tenere un comportamento adeguato per rispettare l'integrità delle attrezzature. A tale scopo è predisposto dal responsabile dei Laboratori un regolamento di comportamento che sarà reso noto agli studenti al primo accesso.

Ad ogni alunno verrà assegnato un proprio account e una password che saranno utilizzati per tutti gli utilizzi didattici dei pc. Di norma ogni alunno creerà una propria cartella da posizionare sul desktop e nella quale conserverà i propri lavori.

3 Istruzione e formazione del personale

Il personale ha ricevuto specifiche istruzioni in merito al comportamento da adottare nell'uso delle dotazioni informatiche messe a loro disposizione. In base alla criticità dei trattamenti effettuati da ciascuna componente, sono stati approntati specifici interventi di formazione.

Articolo VI – MISURE DI TIPO TECNOLOGICO CONNESSE ALL'USO DELLA POSTA ELETTRONICA

Il MIUR mette a disposizione di ogni dipendente una casella personale sul dominio *istruzione.it*. Rimandando ai documenti specifici del MIUR per una visione completa delle politiche di utilizzo adottate dal MIUR, si mettono in evidenza i seguenti punti:

- *E' consentito l'utilizzo del proprio account nel dominio "istruzione.it" a fini privati e personali, purché tale utilizzo non sia causa, diretta o indiretta di disservizi dei sistemi elaborativi e dei servizi di posta elettronica dell'Amministrazione.*
- *Gli utenti del servizio di posta elettronica sono tenuti ad usarlo in modo responsabile, cioè, rispettando le leggi, la presente e altre politiche e procedure del Ministero della Pubblica*

Istruzione e secondo normali standard di cortesia, correttezza, buona fede e diligenza professionale.

- *E' fatto divieto a tutti gli utenti di utilizzare il servizio di posta elettronica per inviare messaggi dannosi, di tipo offensivo o sconveniente, come ad esempio, a titolo non esaustivo, messaggi che riportino contenuti o commenti oltraggiosi su argomenti sessuali, razziali, religiosi, politici, ecc. e comunque ogni altra tipologia di messaggio che possa arrecare danno alla reputazione del Ministero della Pubblica Istruzione.*
- *E' vietato l'uso del servizio di posta elettronica a scopi commerciali o di profitto personale e per attività illegali.*
- *L'Amministrazione registra e conserva, in forma anonima, i dati delle caselle di posta elettronica messe a disposizione dei propri utenti, tramite scrittura in appositi file di log, delle seguenti informazioni minime: mittente del messaggio; destinatario/i; giorno ed ora dell'invio; esito dell'invio.*

Per evitare ogni interferenza con la sfera privata del personale docente e ATA, qualunque comunicazione di interesse amministrativo o di lavoro dovrà avvenire per mezzo delle seguenti caselle di posta elettronica:

Per comunicazioni istituzionali:

catd220001@istruzione.it

catd220001@pec.istruzione.it

Per comunicazioni di carattere informativo, organizzativo e didattico potranno essere utilizzate anche le seguenti caselle di posta elettronica:

dirigente@itemartini.gov.it

vicepresidenza@itemartini.gov.it

prevenzionecorruzione@itemartini.org

La consultazione della posta elettronica da parte dei dipendenti può quindi riguardare:

- caselle personali: su dominio *istruzione.it*, messa a disposizione da parte del MIUR e/o casella personale privata, su altro dominio;
- caselle istituzionali di lavoro suddette.

1 Utilizzo delle Caselle personali

Il personale può consultare in orario di servizio caselle personali per motivi legati alla propria attività lavorativa. La gestione deve essere effettuata tramite servizi di "webmail": non è consentito configurare su computer dell'Istituto appositi programmi tipo Outlook o Thunderbird per gestire le proprie caselle personali (anche per garantire al dipendente la dovuta riservatezza).

Nell'uso di caselle personali all'interno della scuola, al dipendente non è comunque consentito:

- inviare messaggi dannosi, di tipo offensivo o sconveniente, come ad esempio, a titolo non esaustivo, messaggi che riportino contenuti o commenti oltraggiosi su argomenti sessuali, razziali, religiosi, politici, ecc. e comunque ogni altra tipologia di messaggio che possa arrecare danno alla reputazione della Scuola o del MIUR;
- l'uso del servizio di posta elettronica a scopi commerciali o di profitto personale e per attività illegali;
- utilizzare tecniche di "mail spamming" cioè di invio massiccio di comunicazioni a liste di distribuzione extra lavorative o azioni equivalenti.

2 Utilizzo delle Caselle istituzionali di lavoro

Le caselle istituzionali sono gestite dagli incaricati in base ai compiti loro assegnati. In caso di assenza dell'incaricato abituale, questo potrà essere sostituito da altro personale, in base all'organizzazione interna del lavoro disposta da D.S. o D.S.G.A.: quindi tali caselle devono essere utilizzate solo a scopo lavorativo e NON devono essere utilizzate come caselle personali.

Oltre alle disposizioni impartite per l'utilizzo delle caselle personali, si aggiungono le seguenti disposizioni:

- Evitare di aprire messaggi provenienti da mittenti sconosciuti e che contengono allegati

sospetti (file con estensione .exe, .scr, .pif, .bat, .cmd,...). In caso di dubbio consultare un tecnico.

- Nel caso in cui si debba inviare un documento all'esterno dell'Istituto, se non specificamente destinato alla modifica, è preferibile utilizzare il formato *.pdf.
- Evitare che la diffusione incontrollata di "Catene di Sant'Antonio" (messaggi a diffusione capillare e moltiplicata) limiti l'efficienza del sistema di posta.
- Evitare di inviare allegati di dimensioni eccessive (se necessario usare formati compressi come *.zip, *.rar,...)
- L'iscrizione a "mailing list" esterne è concessa solo per motivi professionali, prima di iscriversi occorre verificare in anticipo se il sito è affidabile.
- La casella di posta deve essere mantenuta in ordine.

Articolo VII – SERVIZIO DI POSTA ELETTRONICA @itemartini.org E GOOGLE SUITE FOR EDUCATION

1 Descrizione del servizio

L'Istituto mette a disposizione dei propri docenti, studenti e personale ATA (di seguito indicati utenti) una casella di posta elettronica istituzionale, al fine di migliorare ed ottimizzare la comunicazione da e verso l'istituto e nell'ambito della popolazione studentesca.

Le disposizioni che seguono disciplinano le condizioni di utilizzo del Servizio di Posta Elettronica e delle applicazioni (*Google Suite for education*) ad esso connesse e definisce le modalità di accesso per la fruizione del servizio.

Il servizio è fornito gratuitamente ed è fruibile fino al termine del percorso di studio degli studenti o al termine dell'attività lavorativa presso l'Istituto dei dipendenti.

Studenti, docenti e personale ATA possono accedere attraverso l'apposito link web presente sulla home page del sito <http://www.itemartini.gov.it>. Le caselle di posta e *Google Suite for education* fanno parte del dominio @itemartini.org, di cui l'Istituto è proprietario.

La casella è strettamente personale e non è ammesso l'utilizzo da parte di persone diverse dall'assegnatario, né questi può cederla a terzi.

L'Utente, pertanto, accetta di essere riconosciuto quale autore dei messaggi inviati dal suo account e di essere il ricevente dei messaggi spediti al suo account.

L'Istituto si riserva la facoltà di segnalare alle autorità competenti, per gli opportuni accertamenti ed i provvedimenti del caso, le eventuali violazioni alle condizioni di utilizzo indicate nel presente Regolamento, oltre che alle leggi ed ai regolamenti vigenti.

In caso di violazione delle norme stabilite nel presente regolamento l'Istituto potrà sospendere l'account dell'utente senza alcun preavviso e senza alcun addebito a suo carico e fatta salva ogni altra azione di rivalsa nei confronti dei responsabili di dette violazioni.

2 Modalità di accesso

Premesso che l'Istituto per l'erogazione del servizio utilizza server Google, su tali server ogni utente avrà a disposizione una casella di posta elettronica, oltre la possibilità di utilizzare tutti i servizi aggiuntivi di *Google Suite for education*, previsti dalla convenzione con l'Istituto, senza la necessità di procedere ad alcuna installazione per la loro funzionalità.

L'utente potrà cambiare in ogni momento la password di accesso alla casella di posta elettronica.

Le credenziali di accesso alla posta elettronica e ai servizi *Google Suite for education*, saranno di norma nome.cognome@itemartini.org e password.

3 Regole di utilizzo

Ogni singolo Utente è responsabile dell'attività espletata mediante il proprio account e si impegna ad

adoperarsi attivamente per salvaguardare la riservatezza della propria password ed a segnalare qualunque situazione che possa inficiarla.

L'Utente risponderà personalmente di ogni eventuale danno arrecato a se stesso o a terzi, sollevando contestualmente l'Istituto da ogni responsabilità.

Ciascun Utente si impegna a non utilizzare il servizio per effettuare comunicazioni che arrechino danni o turbative alla rete o a terzi utenti o che violino le leggi ed i regolamenti vigenti. In particolare, in via esemplificativa e non esaustiva, è vietato immettere in rete - attraverso il servizio di posta elettronica - materiale che violi diritti d'autore, o altri diritti di proprietà intellettuale o industriale o che costituisca concorrenza sleale.

L'Utente si impegna ad implementare, sulla propria stazione di accesso alla posta elettronica, tutte quelle misure idonee e necessarie ad evitare, o comunque minimizzare, la divulgazione di virus informatici e simili

4 Obblighi derivanti dall'utilizzo della casella di posta elettronica @itemartini.org e di Google Suite For Education

Gli Utenti prendono atto che è vietato servirsi o dar modo ad altri di servirsi del servizio di posta elettronica e delle applicazioni Google messe a disposizione dall'Istituto per danneggiare, violare o tentare di violare il segreto della corrispondenza e il diritto alla riservatezza.

Gli Utenti si impegnano, inoltre, a non trasmettere o condividere informazioni che possano presentare forme o contenuti di carattere pornografico, osceno, blasfemo, diffamatorio o contrario all'ordine pubblico o alle leggi in materia civile, penale ed amministrativa vigenti.

Gli Utenti si impegnano, altresì, al rispetto delle norme di buon utilizzo del servizio ed in particolare s'impegnano a:

a) non trasmettere, distribuire, condividere o mantenere qualsiasi tipo di materiale che violi qualsiasi legge o regolamento in vigore. Questo include, senza limitazioni, materiale protetto da copyright, marchi registrati, segreti industriali o altre proprietà intellettuali, materiale pornografico, diffamatorio o che costituisce trattamento illecito di dati personali o viola le leggi sul controllo delle esportazioni;

b) non procedere all'invio massivo di mail non richieste (spam). La spedizione di qualsiasi forma di spam attraverso il servizio di posta fornito è proibita. Gli account forniti non possono essere utilizzati per raccogliere risposte a messaggi spediti da altri Internet Service Provider, se questi messaggi violano il presente regolamento.

c) non fare pubblicità a nessun tipo di prodotto o servizio; a non pubblicizzare, trasmettere o altrimenti rendere disponibile qualsiasi tipo di software, programma, prodotto o servizio che viola il presente regolamento o la legge vigente.

L'utente, inoltre, si impegna a non divulgare messaggi di natura ripetitiva ("catene di S. Antonio") anche quando il contenuto sia volto a segnalare presunti o veri allarmi (esempio: segnalazioni di virus); a fronte di tale evenienza l'utente è tenuto a segnalarla al servizio assistenza.

5 Norme finali

L'Istituto si riserva il diritto di sospendere temporaneamente l'utilizzo del servizio di posta o di revocarlo definitivamente qualora si verificassero violazioni del presente Regolamento.

L'Istituto si impegna a tutelare i dati forniti dall'utente in applicazione del D.Lgs. n. 196/2003 "Codice in materia di protezione dei dati personali".

Articolo VII – MISURE DI TIPO TECNOLOGICO CONNESSE ALL'USO DI INTERNET

Regole da osservare nell'uso di Internet

Al fine di ridurre il rischio di usi impropri della "navigazione", dovranno essere rispettate le seguenti disposizioni:

1. Al personale non è consentito:
 - servirsi o dar modo ad altri di servirsi della stazione di accesso a internet per attività non istituzionali, per attività poste in essere in violazione del diritto d'autore o altri diritti tutelati

- dalla normativa vigente;
 - utilizzare sistemi *Peer to Peer* (P2P), di file sharing, podcasting, webcasting social network o similari (salvo specifiche attività espressamente autorizzate per le finalità istituzionali).
2. Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico mediante virus o mediante ogni altro software aggressivo (attenzione nell'aprire mail e relativi allegati, non navigare su siti poco professionali, ecc..)
 3. Ogni utente è tenuto a controllare la presenza e il regolare funzionamento del software antivirus, segnalando ogni eventuale problema all'amministratore di sistema.
 4. Nei sistemi nei quali si è avuto accesso per mezzo di credenziali personali (postazioni di segreteria, PC collegati alle LIM) è responsabilità dell'utente, al termine delle operazioni, effettuare l'operazione di log-out nel momento in cui si abbandona, anche temporaneamente, la postazione per evitare che possano avere accesso ai sistemi persone non autorizzate.

Sistema di gestione degli utenti e degli accessi ad Internet

Per garantire la sicurezza informatica ed il controllo del corretto utilizzo dell'accesso ad Internet l'Istituto si è dotato di strumenti specifici che consentono:

- la protezione da accessi non autorizzati provenienti da Internet
- controlli antivirus centralizzati
- di bloccare l'accesso ai siti presenti in una black list costantemente aggiornata
- la conservazione in un file di informazioni relative alla navigazione in Internet come, ad esempio, utente, PC, ora di accesso, pagine accedute, etc.

Gli alunni non possono avere accesso alla rete wifi dell'istituto se non per l'attuazione di specifici progetti volti all'uso delle nuove tecnologie nella didattica per i quali potranno essere autorizzati dalla Dirigenza Scolastica e abilitati, anche solo per specifiche fasce orarie.

Le informazioni lasciate sui sistemi di controllo degli accessi ad Internet come quelle lasciate da ciascun utente sui PC, sui server e sui programmi impiegati, potranno essere utilizzate per individuare e sanzionare eventuali comportamenti non conformi al presente regolamento.

La conservazione nel tempo dei dati relativi all'uso degli strumenti informatici verrà fatta per il periodo strettamente limitato al perseguimento di finalità organizzative, produttive e di sicurezza ovvero in adempimento di obblighi previsti dalla legge;

Streaming e scaricamento di grandi quantità di dati

Si ricorda poi che scaricare file audio e video (o comunque grandi quantità di dati) è in grado di degradare le prestazioni offerte dal servizio agli altri utenti: per tale motivo ciò può avvenire solo se necessario e, possibilmente, al di fuori dei momenti "di punta" a livello di Istituto.

Articolo VIII – SOCIAL MEDIA POLICY

1 Parte generale

L'Istituto, per costruire nuove modalità di interazione e partecipazione, ha aggiunto al sito istituzionale della scuola www.itemartini.gov.it i seguenti spazi sulle principali piattaforme di social media network:

- una pagina Facebook <https://www.facebook.com/itemartini>
- l'account Twitter @itemartini <https://twitter.com/itemartini>
- l'account You Tube <https://www.youtube.com/itemartini>

Questi spazi permettono di promuovere e informare sulle attività scolastiche e sulle risorse didattiche disponibili, favorendo la comunicazione, la trasparenza e le conversazioni digitali fra le diverse componenti della comunità scolastica (docenti, studenti, genitori, dirigenza, personale amministrativo) in un'ottica partecipata e collaborativa, di apertura e condivisione dei dati e delle informazioni.

La **social media policy** descrive le regole di comportamento ("Netiquette") che gli utenti sono invitati a osservare nell'interazione con le pagine e i profili dell'ITE "P. Martini" sui social network e nell'uso degli strumenti social presenti nei siti web associati.

Le presenti indicazioni (redatte in conformità a quanto disposto dalle "Linee Guida per i siti web della PA – Vademecum Pubblica Amministrazione e social media" del Ministero della Funzione Pubblica)

hanno carattere orientativo, ferma restando la responsabilità personale nel caso di violazione delle leggi italiane, anche sulla rete. Esse hanno anche lo scopo di fornire alle componenti scolastiche linee di comportamento per un uso critico, consapevole e responsabile dei social media. Educare gli adolescenti all'uso dei social media non serve solo a contrastare il cyberbullismo, ma anche ad accrescere la consapevolezza sulla cautela nel condividere le proprie informazioni in rete.

2 Responsabili della gestione dei social network

Gli account (pagine e profili) istituzionali dell'Istituto e gli strumenti social presenti nei siti web associati sono amministrati da un team per la comunicazione esterna, di cui è responsabile il Dirigente Scolastico.

3 Finalità

L'Istituto utilizza i principali social network nel rispetto del Regolamento di Istituto, delle altre disposizioni amministrative e delle norme di legge; in questi spazi l'Istituto intende perseguire finalità istituzionali e di interesse generale. Gli account istituzionali dell'Istituto sui social network e gli strumenti social presenti nei siti web associati si propongono come luoghi di informazione, comunicazione e condivisione con l'utenza, il territorio, le istituzioni, i media.

4 Contenuti

Attraverso gli account istituzionali dell'Istituto sui social network sono pubblicati contenuti (notizie, comunicati, aggiornamenti di stato, contenuti testuali, collegamenti ad altri contenuti, materiale infografico, fotografico, audiovisivo ecc.) di attinenza agli scopi istituzionali dell'Istituto. I contenuti, se non diversamente specificato, sono da considerarsi rilasciati secondo la licenza [**Creative Commons CC BY NC SA**](#) (Attribuzione – Non commerciale - Condividi allo stesso modo 3.0 Italia).

Sfruttando le opportunità tipiche dei social network, l'Istituto può condividere e rilanciare contenuti di pubblico interesse e utilità realizzate da soggetti terzi. Pur verificandone per quanto possibile la precisione e l'attendibilità, la scuola non assume alcuna responsabilità per eventuali informazioni errate o non aggiornate.

La presenza di spazi pubblicitari a margine dei contenuti pubblicati nelle pagine dei social network utilizzati non è sotto il controllo dell'Istituto, ma è gestita in autonomia dagli stessi social network.

5 Comportamenti consentiti agli utenti sui social network

Tutti hanno il diritto di interagire con gli account istituzionali dell'Istituto intervenendo con commenti e proponendo contenuti che siano espressione della propria libera opinione, nel rispetto delle opinioni altrui.

I commenti e i post degli utenti rappresentano l'opinione dei singoli e non quella dell'Istituto, che non può essere ritenuto responsabile della veridicità o meno di ciò che viene postato sui canali da terzi.

L'Istituto, invitando a una conversazione educata, pertinente e rispettosa, si impegna a gestire spazi di comunicazione e dialogo all'interno dei propri profili, nei diversi social network, chiedendo alle componenti scolastiche il rispetto di alcune regole d'uso.

Nel caso di social network che, come Facebook, danno accesso a informazioni relative alla vita privata, si raccomanda di valutare attentamente il tipo di informazioni da immettere sulla rete, a salvaguardia della libertà e della necessaria riservatezza di tutti i soggetti. Funzioni come la geolocalizzazione o foto a carattere personale possono generare situazioni inopportune (ad esempio in caso di assenze, giustificazioni, ecc.).

Nei social network ognuno è responsabile dei contenuti che pubblica e delle opinioni che esprime; è opportuno ricordare che ciò che viene pubblicato, spesso, rimane in rete anche se viene apparentemente rimosso. Gli insegnanti e il personale ATA dell'Istituto sono invitati a tenere presente che qualsiasi opinione esprimano sui social network può danneggiare la reputazione e la credibilità dell'Istituto con conseguenti ricadute di carattere disciplinare.

6 Comportamenti non consentiti agli utenti dei social network

L'utente è responsabile dei contenuti che pubblica e delle opinioni espresse. Non è consentito l'utilizzo del servizio per effettuare comunicazioni che violino le leggi vigenti, e in particolare per l'invio di messaggi che possano presentare forme o contenuti di carattere osceno, blasfemo, discriminatorio, diffamatorio o comunque tale da offendere la morale comune e la sensibilità degli utenti. Non sono consentiti atteggiamenti discriminatori rispetto al genere, orientamento sessuale, età, religione, convinzioni personali, origini etniche e disabilità. Non sono consentiti comportamenti gratuitamente polemici e reiterati («trolling» e «flame»).

I contenuti pubblicati hanno il requisito dell'interesse pubblico, per cui non è ammessa alcuna forma di spam, pubblicità o promozione di interessi privati, raccolta fondi, violazione del diritto d'autore, utilizzo non autorizzato di marchi registrati e sostegno ad attività illegali.

I contenuti devono rispettare la privacy delle persone, evitando riferimenti a fatti o a dettagli privi di

rilevanza pubblica e messaggi contenenti la diffusione non autorizzata di dati personali di terzi (indirizzi, email, numeri telefonici ecc.). L'autore di un errore deve essere pronto a modificare il suo intervento, appena la violazione gli viene segnalata. Un intervento inappropriato, se non rimosso prontamente, può dare origine a conseguenze anche di ordine penale. I giudizi di rimozione di post, commenti o altri contenuti sono insindacabili.

Non è consentito al personale docente e Ata in orario di servizio utilizzare i Social Network quali Twitter, Facebook, etc. salvo specifiche attività espressamente autorizzate dal dirigente scolastico per le finalità istituzionali.

7 Moderazione

La moderazione da parte dell'Istituto all'interno dei propri spazi social avviene a posteriori, ovvero in un momento successivo alla pubblicazione, ed è finalizzata unicamente al contenimento, nei tempi e nei modi ragionevolmente esigibili, di eventuali comportamenti contrari alle norme d'uso.

Gli amministratori hanno facoltà di eliminare senza preavviso i contenuti non conformi e contrari alle regole descritte in questa policy. Un utente che reiteratamente non rispetta le regole descritte potrà essere bloccato e i contenuti potrebbero, se necessario, essere segnalati alle autorità competenti.

Gli amministratori hanno comunque facoltà di rimuovere eventuali contenuti non attinenti alle attività dell'Istituto, né agli argomenti di attualità o di interesse generale ad esse correlati.

Articolo IX – TRATTAMENTI ESCLUSI

L'Istituto non effettua controlli prolungati, costanti o indiscriminati dell'uso di Internet e Posta elettronica da parte dei dipendenti.

L'Istituto non effettua trattamenti di dati personali mediante sistemi hardware e software che mirano al controllo a distanza di lavoratori attraverso:

- lettura e registrazione sistematica dei messaggi di posta elettronica personali dei dipendenti o dei relativi dati esteriori;
- riproduzione ed eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore;
- lettura e registrazione dei caratteri inseriti dai lavoratori tramite la tastiera ovvero dispositivi analoghi a quello descritto.

Articolo X – GRADUALITÀ DEI CONTROLLI

Nel caso in cui un evento dannoso o una situazione di pericolo non sia stato impedito con preventivi accorgimenti tecnici, il Dirigente Scolastico può adottare eventuali misure che consentano la verifica di comportamenti anomali.

Per quanto possibile, sarà preferito un controllo preliminare su dati aggregati, riferiti all'intera struttura lavorativa o a sue aree. Il controllo anonimo può concludersi con un avviso generalizzato relativo ad un rilevato utilizzo anomalo degli strumenti d'Istituto e con l'invito ad attenersi scrupolosamente a compiti assegnati e istruzioni impartite. L'avviso può essere circoscritto a dipendenti afferenti all'area o settore in cui è stata rilevata l'anomalia.

La presenza di successive anomalie potrà comportare controlli su base individuale.

La rilevazione delle anomalie e delle verifiche tecniche è a cura dell'Amministratore di Sistema che potrà anche intervenire su richiesta del Dirigente Scolastico per la verifica di situazioni anomale o sospette.

Responsabile dei successivi e consequenziali provvedimenti è il Dirigente Scolastico.

Articolo XI – SANZIONI

È fatto obbligo a tutti i Lavoratori di osservare le disposizioni del presente disciplinare e qualunque altra comunicata dall'Amministrazione in materia di sicurezza e gestione delle attrezzature informatiche.

Il mancato rispetto o la violazione delle regole contenute nel presente Disciplinare è perseguibile con tutte le azioni civili e penali previste dalla legge, nonché con i provvedimenti disciplinari, in conformità a quanto previsto dalle disposizioni normative e contrattuali vigenti per il personale. Rimane ferma ogni ulteriore forma di responsabilità civile e penale, quali ad es.:

- violazione della privacy e della tutela dell'immagine;
- diffamazione;
- accesso abusivo ad un sistema informatico e telematico;
- violazione della legge sul copyright.

Il codice di comportamento ed il codice disciplinare sono consultabili nel sito internet dell'Istituto www.itemartini.gov.it e nell'Albo On Line dello stesso sito.

Articolo XII – DISPOSIZIONI ULTERIORI

I dati personali inerenti i Lavoratori non possono essere portati a conoscenza di terzi non autorizzati. I colleghi di lavoro della persona interessata sono considerati terzi.

L'Amministrazione, nell'ambito di procedimenti disciplinari e/o di procedimenti penali di cui all'art. XII del presente Disciplinare e nel rispetto del principio di protezione dei dati personali e del divieto di controllo a distanza del Lavoratore, procede alla conservazione delle "registrazioni a giornale" (log file) relative all'utilizzazione di Internet e/o della Posta Elettronica o/e dei files delle telefonate e/o dei Fax e dei Fax mail, fino alla conclusione dei relativi procedimenti.

Il presente documento, che costituisce parte integrante e sostanziale del Regolamento di Istituto, viene portato a conoscenza di tutti i Lavoratori, indicati all'art. IV del presente Disciplinare, mediante pubblicazione nella sezione Albo On Line del sito internet istituzionale www.itemartini.gov.it.

Articolo XIII – AGGIORNAMENTO PERIODICO, ENTRATA IN VIGORE E PUBBLICITA'

Il presente regolamento è aggiornato con cadenza almeno annuale o in caso di rinvenimento di soluzioni tecnologiche ritenute più idonee a tutelare i dati personali dei lavoratori, e portato a conoscenza di tutti i lavoratori mediante affissione all'albo dell'istituto.

Con l'entrata in vigore del presente regolamento tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalle presenti.

Copia del regolamento, oltre ad essere pubblicata all'albo on line dell'Istituto, verrà consegnato individualmente a ciascun utente informatico di segreteria.