ISTITUTO di ISTRUZIONE SECONDARIA SUPERIORE
MARIE CURIE
• LICEO SCIENTIFICO
• TECNICO TECNOLOGICO
• PROF. LE INDUSTRIA E ARTIGIANATO

SAVIGNANO sul RUBICONE (FC)
Via Togliatti n.5 C.A.P. 47039
Tel. 0541 944602
Fax 0541 941481
C.F. 90038920402
Mail: fois001002@istruzione.it
P.E.C. fois001002@pec.istruzione.it
Web site: www.mcurie.gov.it

Prot.n. 3686/C14 Savignano sul Rubicone, 11/08/2014

REGOLAMENTO INTERNO SULL'UTILIZZO DI INTERNET E DELLA CASELLA DI POSTA ELETTRONICA ISTITUZIONALE SUL LUOGO DI LAVORO

IL DIRIGENTE SCOLASTICO

VISTO il Decreto Legislativo 30 giugno 2003, n. 196 recante "Codice in materia di protezione dei dati personali" e s.m.i.;

VISTO il Provvedimento del Garante per la Protezione dei Dati Personali 1 marzo 2007 n. 13 (in G.U. n. 58 del 10 marzo 2007);

VISTA la Direttiva del Dipartimento della Funzione Pubblica 26 maggio 2009, n. 2;

VISTO il D.P.R. 16 aprile 2013 n. 62 recante il nuovo Codice di comportamento dei dipendenti pubblici a norma dell'articolo 54 del decreto legislativo 30 marzo 2001, n. 165;

VISTO l'art. 92 del CCNL 2007 Capo IX – Norme disciplinari – Obblighi del dipendente,

VISTO D.Lgs. 27 ottobre 2009, n.150;

VISTA la deliberazione del CNIPA 19/12/2004 n. 11 "Regole tecniche dei documenti digitali";

VISTO il D. Lgs. 7 marzo 2005 n. 82 "Codice dell'Amministrazione Digitale";

VISTO il D. Lgs. 159 del 4/4/2006 recante "Disposizioni integrative e correttive al D.Lgs. 7/3/2005 n.82;

VISTA la legge 20 maggio 1970 n. 300 "Statuto dei Lavoratori";

CONSIDERATO:
- che l'istituzione scolastica, quale datore di lavoro, nella persona del dirigente scolastico pro tempore, è tenuta ad assicurare la funzionalità ed il corretto impiego degli strumenti I.C.T. (Information & Communication Technologies, ovvero Tecnologie dell'Informazione e della Comunicazione) da parte dei propri dipendenti, definendone le modalità di utilizzo nell'organizzazione dell'attività lavorativa ed adottando le misure necessarie a garantire la sicurezza, la disponibilità e l'integrità dei sistemi informativi;

- che a fronte del potere di controllo dell'Amministrazione datore di lavoro, esiste in capo ai dipendenti l'obbligo, sancito da norme di legge, anche di rilevanza penale, e di contratto, di adottare comportamenti conformi al corretto espletamento della prestazione lavorativa ed idonei a non causare danni o pericoli ai beni mobili ed agli strumenti ad essi affidati, tra i quali vi sono le attrezzature I.C.T. ed i sistemi informativi messi a disposizione dall'Amministrazione;

- che il datore di lavoro, secondo i poteri a lui affidati dalle norme del codice civile, articoli 2086, 2087 e 2104, può riservarsi di controllare l'effettivo adempimento della prestazione lavorativa ed il corretto utilizzo degli strumenti di lavoro; nell'esercizio di tali prerogative, tuttavia, deve rispettare la libertà e

la dignità dei lavoratori, tenendo presente, al riguardo, quanto disposto dalle norme poste a tutela del lavoratore;

- che l'Amministrazione, tenendo conto delle peculiarità proprie di ciascuna organizzazione ed articolazione di uffici ed, eventualmente, anche dei diversi profili professionali autorizzati all'uso della rete, potrà adottare una o più delle misure indicate dalla deliberazione del Garante della privacy 01 marzo 2007 n. 13;

RICHIAMATO il principio generale che l'utilizzo delle risorse informatiche e della rete che la scuola mette a disposizione del personale deve sempre ispirarsi a criteri di diligenza e correttezza che sono normalmente adottati nell'ambito dei rapporti di lavoro;

CONSIDERATO che, se correttamente applicato e fatto rispettare, il presente regolamento è da intendersi quale strumento della Policy scolastica anche al fine di limitare il rischio di insorgenza di responsabilità amministrativa dell'Istituto;

RITENUTO pertanto di dover avviare l'apposita regolamentazione per l'utilizzo di Internet e della Posta Elettronica in cui 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 commi 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;

- in qualità di Titolare del trattamento dei dati personali di questa Istituzione scolastica,

A D O T T A

il presente regolamento, avente ad oggetto la precisa definizione di criteri e modalità di accesso ed utilizzo ai servizi Internet e posta elettronica da parte del personale dipendente dell'Istituto di Istruzione Secondaria "Marie Curie" di Savignano sul Rubicone.

Il presente regolamento intende porre in essere ogni dispositivo necessario ai fini di disciplinare la gestione e l'utilizzo della navigazione in Internet e del servizio di posta elettronica dell'I.I.S.S. "M.Curie" mediante PC, portatili e tablets messi a disposizione dell'Amministrazione e mediante portatili e/o tablets personali, nonché l'uso dei telefoni aziendali e dei fax.

Il presente dispositivo si applica a tutto il personale senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori, interni o esterni, dell'Istituto, agli esperti esterni, ai collaboratori a progetto e a quelli che intrattengono rapporti con l'Istituto durante il periodo di stage, a prescindere dal rapporto contrattuale con la stessa intrattenuto.

Art. 1 - Modalità di utilizzo delle postazioni di lavoro

L'accesso alla rete internet è concessa ai dipendenti quali utenti autenticati e nei limiti stabiliti per ciascun profilo di utenza, così come indicati nelle relative lettere di incarico e nell'informativa loro rilasciata ai sensi dell'art. 13 del D.Lgs. n. 196 del 2003.

La corretta navigazione in Internet e il sistema di posta elettronica sono mezzi di comunicazione, informazione e trasmissione di dati. I dati che vengono inviati e ricevuti con tale sistema sono di esclusiva proprietà dell'Istituzione Scolastica.

Tutte le attività svolte mediante la navigazione in Internet e il sistema di posta elettronica sono finalizzate al conseguimento dei fini istituzionali dell'Istituzione Scolastica.

I computer dell'Istituto sono affidati al personale come strumento di lavoro.

Per quanto riguarda il personale amministrativo e tecnico, ogni dipendente riceve indicazione della postazione di lavoro a lui assegnata al momento della presa di servizio, ovvero in caso di cambiamento della propria postazione.

Ciascun dipendente a seconda delle necessità potrà operare su altro PC non direttamente assegnato, usando sempre le proprie credenziali di accesso personale (nome utente e password) senza creare ulteriori account.

L'accesso ad Internet da parte del personale tecnico, docente e degli studenti potrà avvenire nelle classi, nei laboratori, in biblioteca, e in qualunque altro luogo a tale attività destinato, sempre mediante le proprie personali credenziali di accesso (nome utente e password) e solo per scopi didattici .

L'accesso alle postazioni di lavoro di segreteria e ai servizi informativi è protetto tramite sistema di autenticazione che richiede l'immissione di un apposito codice utente e della relativa password.

La gestione degli utenti avviene in maniera centralizzata sul server di segreteria su cui è configurato un dominio in ambiente Windows server e nel quale potranno quindi essere conservate informazioni relative agli accessi dei singoli utenti.

Le modalità relative al rilascio e alla gestione delle credenziali di autenticazione sono indicate al successivo art. 2.

Ogni utente è responsabile per il proprio account e per l'uso che ne viene fatto, essendo tenuto a tutelarlo da accessi non autorizzati. Non è ammessa la comunicazione del proprio account a terzi.

Analogo sistema di gestione è garantito per gli utenti relativi all'attività didattica (alunni, docenti e personale tecnico) sulla rete didattica d'istituto.

Relativamente all'utilizzo dei singoli PC affidati agli utenti, l'assegnazione delle risorse non ne comporta la privatezza, in quanto trattasi di strumenti di esclusiva proprietà dell'Istituto scolastico.

Ognuno è responsabile dell'utilizzo delle dotazioni informatiche, fisse o mobili, ricevute in assegnazione o comunque disponibili nell'istituto scolastico.

E' vietato servirsi, o dar modo ad altri di servirsi, della postazione di accesso a internet per attività non istituzionali, per attività poste in essere in violazione del diritto d'autore, altri diritti tutelati dalla normativa vigente o in violazione di norme di legge o di regolamento.

Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico mediante virus o mediante ogni altro software aggressivo. Per questo motivo è necessario porre cautela nel navigare su siti poco professionali.

Gli utenti che utilizzano le postazioni informatiche di lavoro devono:

A. mantenere la corretta configurazione del proprio computer non alterando le componenti hardware e software predisposte allo scopo, né installando ulteriori software non autorizzati;
B. non connettere in rete stazioni di lavoro se non dietro esplicita autorizzazione del Dirigente Scolastico e dell'amministratore di sistema;
C. è consentito salvare su server e computer dell'Istituto solo dati di carattere lavorativo, in quanto ai dati salvati su computer dell'Istituto potrebbero accedere altri dipendenti, in base a competenze e funzioni;
D. prestare la massima attenzione ai supporti di origine esterna (es. pen drive), verificando preventivamente tramite il programma di antivirus ogni file acquisito attraverso qualsiasi supporto e avvertendo immediatamente gli assistenti tecnici e/o l'Amministratore di Sistema nel caso in cui vengano rilevati virus o eventuali malfunzionamenti;
E. spegnere il PC al termine del turno di lavoro o in caso di assenze prolungate dalla propria postazione.

Vanno evitati utilizzi non inerenti all'attività lavorativa, che possono inoltre contribuire a innescare disservizi, costi di manutenzione e minacce alla sicurezza.

Per gli utenti che accedono a Internet è vietato:

1. la visione di siti non pertinenti alla attività lavorativa;
2. l'utilizzo di servizi di rete non correlati alla attività lavorativa;
3. caricare/scaricare (upload/download) a/da Internet di files musicali, immagini, video o software non inerenti alla attività lavorativa;
4. l'uso dei servizi di rete con finalità ludiche, di gioco o ricreative, diversi da quelli in uso o comunque estranei all'attività lavorativa;
5. scaricare e masterizzare su archivi personali dati e immagini non inerenti alla funzione pubblica;
6. reiterare tentativi di accesso a siti bloccati e di cui si è avuta evidenza del fatto che si tratta di siti non appropriati e non consentiti;
7. servirsi delle postazioni di accesso a Internet per attività non istituzionali e non connesse ad attività lavorative e per attività poste in essere in violazione del diritto d'autore, altri diritti tutelati dalla normativa vigente o in violazione di norme di legge o di regolamento;
8. registrarsi a siti i cui contenuti non siano connessi all'attività lavorativa;
9. accedere a siti pornografici, di intrattenimento, ecc.
10. utilizzare sistemi di chat non previamente autorizzati e non correlati a finalità istituzionali.

Tenuto conto di quanto sopra richiamato si fa presente che scaricare file audio e video, o comunque grandi quantità di dati, concorre a degradare le prestazioni offerte dal servizio agli altri utenti.

E' vietato l'utilizzo delle risorse del server centrale per la memorizzazione di materiale privato, personale o non attinente all'attività lavorativa.

L'Ufficio tecnico è tenuto a controllare la presenza e il regolare funzionamento del software antivirus, segnalando ogni eventuale problema al Dirigente Scolastico.

Tutti i dipendenti sono tenuti ad adottare un comportamento conforme al corretto espletamento della propria attività lavorativa ed idoneo a non causare danni o pericoli ai beni mobili, agli strumenti e ai sistemi informativi messi a disposizione dall'istituto scolastico.

Tutti i dipendenti sono tenuti ad attenersi agli obblighi di assoluta riservatezza connessi al proprio incarico e di impegnarsi a rispettare il divieto assoluto di comunicare e diffondere, nel corso e alla cessazione dell'incarico stesso, senza limiti temporali, a terzi non autorizzati, le informazioni di cui sia venuto a conoscenza, siano essi rappresentati da dati, procedure, programmi, archiviazione, conservazione dei dati, od altro, di proprietà dell'Istituto, senza specifica autorizzazione scritta del Dirigente Scolastico.

Tutti i dipendenti sono tenuti ad informare il Dirigente Scolastico qualora si verificasse la necessità di porre in essere operazioni per finalità o con modalità diverse da quelle risultanti dalle istruzioni ricevute.

Tutti i dipendenti sono tenuti a rispettare ed applicare le misure di sicurezza idonee a salvaguardare la riservatezza e l'integrità dei dati trattati durante l'utilizzo delle postazioni di lavoro.

E' fatto assoluto divieto di portare le attrezzature tecnologiche di proprietà dell'istituzione scolastica al di fuori dei locali della scuola, per uso privato.

Art. 2 - Modalità relative al rilascio, alla gestione e alla corretta conservazione delle credenziali di autenticazione

L'accesso alle postazioni di lavoro e ai servizi informativi è protetto mediante l'uso di credenziali di autenticazione personali, basate sul meccanismo di "username e password", rilasciate nel rispetto del

D. Lgs. n. 196/2003, con riferimento al disciplinare tecnico in materia di misure minime di sicurezza. Tali credenziali vengono rilasciate, previa identificazione fisica dell'utente, dal Dirigente Scolastico, da uno dei suoi collaboratori all'uopo delegati, o dal Direttore dei Servizi Generali e Amministrativi.

Il sistema di autenticazione informatica consente il trattamento dei dati solo agli Incaricati in possesso di Codice Identificativo (UserID) e Parola Chiave(Password), oppure di dispositivo di autenticazione. In alcuni casi la procedura di registrazione consente di inserire i propri dati anagrafici ed ottenere direttamente le credenziali di accesso, accompagnate da un codice PIN che viene successivamente inviato a mezzo e-mail.

L'username o UserID prevede criteri di definizione, di assegnazione e di disattivazione, è a carattere individuale, non è riutilizzabile e ha validità limitata nel tempo.

La Password prevede criteri di creazione e di custodia, validità temporale e modalità di ripristino in caso di perdita.

Ogni incaricato può ricevere una o più credenziali di accesso ai vari sistemi, ciascuna riferita a diversi profili di autenticazione, generati dal responsabile o da un collaboratore del dirigente, in accordo con il Titolare del trattamento dati, per svolgere i compiti propri delle designazioni d'incarico mediante strumenti informatici.

La Password legata all'username UserId, consente la riconoscibilità personale. La prima password generata e comunicata, ha validità temporanea e deve essere cambiata al primo accesso.

La gestione delle Password prevede alcune regole fondamentali:

1) la password deve essere cambiata dallo stesso incaricato,
2) deve essere costituita di almeno otto caratteri alfanumerici,
3) non deve contenere il nome e/o il cognome e/o data di nascita o indirizzi dell'utente, del coniuge, dei figli, la posizione lavorativa o il nome della scuola o dell'ufficio,
4) non deve essere una parola di senso compiuto,
5) non devono essere usati termini comuni come "password", "accesso", "12345678" o "qwertyui" (i primi otto caratteri alfabetici della tastiera),
6) non può essere una delle ultime tre password utilizzate,
7) non può contenere il proprio account,
8) deve contenere alternati almeno tre dei seguenti quattro gruppi di caratteri:
   a. caratteri dell'alfabeto maiuscoli (A-Z),
   b. caratteri dell'alfabeto minuscoli (a-z),
   c. numeri (0-9)
   d. caratteri non alfabetici (!, $, #, %, ecc.)

Incaricati con le stesse mansioni ed attività utilizzano UserId e password diverse e personali.
L'accesso con UserId e Password viene garantito anche da postazioni diverse da quelle di utilizzo personale.
E' obbligatorio sospendere manualmente la sessione d'uso di sistema operativo quando ci si allontana dalla postazione.
Delle proprie credenziali di accesso e delle password assegnate è responsabile l'utente assegnatario.
L'utente è informato del fatto che la conoscenza delle proprie credenziali da parte di terzi consentirebbe a questi ultimi l'utilizzo del servizio in nome dell'utente medesimo. L'utente è il solo ed unico responsabile della conservazione e della riservatezza delle proprie credenziali e, conseguentemente, rimane il solo ed unico responsabile per tutti gli usi ad essa connessi o correlati, ivi compresi danni e conseguenze pregiudizievoli arrecati al'I.I.S.S. Marie Curie e/o a terzi, siano dal medesimo utente autorizzati ovvero non autorizzati.
L'utente, ha l'obbligo di osservare la seguente politica di gestione delle credenziali che la scuola ha adottato per garantire una corretta conservazione delle stesse:

a) conservare nella massima riservatezza e con la massima diligenza le parole di accesso alla rete, ai sistemi, e qualsiasi altra informazione legata a processi di autenticazione personale;

b) le password non devono mai essere lasciate incustodite e conoscibili a terzi;

c) ciascuno è responsabile della custodia delle proprie credenziali identificative;

d) le password fornite sono a carattere assolutamente personale, non sono cedibili ad altri e possono essere utilizzate esclusivamente per finalità di lavoro;

e) l'eventuale furto, smarrimento o perdita della password deve essere comunicato tempestivamente al Dirigente Scolastico o ad uno dei suoi collaboratori; in ogni caso, l'utente è responsabile delle conseguenze derivanti dal furto, dalla perdita o dallo smarrimento delle credenziali;

f) non lasciare incustodita ed accessibile la propria postazione una volta connesso al sistema con le proprie credenziali di autenticazione, provvedendo a bloccare la postazione in caso di allontanamento temporaneo;

g) non cedere, una volta superata la fase di autenticazione, l'uso della propria postazione a persone non autorizzate, in particolar modo per quanto riguarda l'accesso a Internet ed ai servizi di posta elettronica;

h) non utilizzare credenziali (user-id e password) di altri utenti, nemmeno se fornite volontariamente o di cui si ha casualmente conoscenza;

i) al fine di evitare il fenomeno del *"phishing mail"* contenenti link a siti che mirano ad estorcere le credenziali di accesso dei vari sistemi informatici, non fornire per alcun motivo le password su siti raggiunti tramite i predetti link; qualora vengano inavvertitamente fornite le credenziali a seguito di ricezione di mail appartenenti a tale tipologia, effettuare tempestivamente il cambio della password al fine di impedirne l'illecito utilizzo.

Tutte le attività svolte in sessione d'uso sono direttamente riconducibili alla credenziale di accesso attribuita al singolo Incaricato, che rispetto al suo operato, si assume ogni responsabilità.

Le credenziali sono assegnabili o rinnovabili a discrezione del Dirigente Scolastico solo a chi è in possesso di un contratto di lavoro subordinato o di collaborazione con l'istituzione scolastica.

Le credenziali sono sottoposte ad una data di scadenza che può variare da categoria a categoria e sono mantenute attive fino a cessazione dell'incarico presso l'Istituto Marie Curie.

Art. 3 - Utilizzo della Posta Elettronica

L'utilizzo di posta elettronica è consentito solo per motivi istituzionali e connessi all'attività lavorativa, da parte di dipendenti ai quali è stata assegnata un'utenza di posta individuale relativa all'ufficio.

L'accesso è consentito in via esclusiva ai dipendenti ai quali sono state comunicate credenziali di autenticazione per l'accesso alla casella di posta.

All'utente di posta elettronica è vietato:

- trasmettere materiale commerciale e/o pubblicitario non richiesto (spamming), nonché permettere che le proprie risorse siano utilizzate da terzi per questa attività;

- prendere visione della posta altrui e simulare l'identità di un altro utente, ovvero utilizzare per l'invio di messaggi credenziali di posta non proprie, nemmeno se fornite volontariamente o di cui si ha casualmente conoscenza;

- trasmettere a mezzo posta elettronica dati sensibili, personali o commerciali di alcun genere se non nel rispetto delle norme sulla disciplina del trattamento della protezione dei dati;

- l'uso della posta elettronica non è comunque consentito per partecipare a forum e/o dibattiti se non per motivi istituzionali, per diffondere notizie non veritiere o quanto altro che abbia contenuto offensivo e discriminatorio, per inviare lettere a catena ovvero messaggi ripetuti.

All'interno della segreteria sono attivati indirizzi di posta elettronica condivisi dagli uffici, assegnati a ciascun dipendente per opportunità lavorativa.

La "personalizzazione" dell'indirizzo non comporta la sua "privatezza", in quanto trattasi di strumenti di lavoro di esclusiva proprietà dell'Istituto, messi a disposizione del dipendente al solo fine dello svolgimento delle proprie mansioni lavorative.

Le caselle istituzionali PEO fois001002@istruzione.it e PEC fois001002@pec.istruzione.it 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.. Tali caselle devono essere utilizzate solo a scopo lavorativo e, analogamente alla navigazione su internet, non devono essere utilizzate come caselle private.

Gli utenti hanno l'obbligo di procedere alla tempestiva lettura della corrispondenza pervenuta nella propria casella di posta elettronica almeno una volta al giorno. Parimenti, hanno l'obbligo di non cedere ad altri la propria password di cui sono gli unici responsabili e di sostituirla periodicamente, nel rispetto del D. Lgs. 196/2003 con le modalità ed i tempi in esso riportati.

Il personale può consultare in orario di servizio le caselle personali per motivi legati alla propria attività lavorativa. La gestione deve essere effettuata tramite servizi di "webmail", anche per garantire al dipendente la dovuta riservatezza.

Gli utenti del servizio di posta elettronica sono tenuti ad usarlo in modo responsabile, cioè rispettando le leggi, il presente regolamento e le politiche e le procedure del Ministero Istruzione, Università e Ricerca, secondo normali standard di cortesia, correttezza, buona fede e diligenza professionale.

E' fatto divieto a tutti gli utenti di utilizzare o alterare il servizio di posta elettronica per inviare messaggi dannosi, di tipo offensivo o sconveniente, razzista o diffamatorio come ad esempio, a titolo non esaustivo, messaggi che riportino contenuti o commenti oltraggiosi e, comunque, ogni altra tipologia di messaggio che possa arrecare danno all'immagine della scuola e alla reputazione del M.I.U.R.

E' vietato l'uso del servizio di posta elettronica a scopi commerciali o di profitto personale e per attività illegali e utilizzare tecniche di "mail spamming", cioè di invio massiccio di comunicazioni a liste di distribuzione extra lavorative o azioni equivalenti.

Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico mediante virus o mediante ogni altro software aggressivo, per questo è necessario porre cautela nell'aprire e-mail sospette e relativi allegati.

Il personale è invitato a:

- 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 è opportuno consultare un tecnico;
- al fine di evitare il fenomeno del *"phishing mail"* contenenti link a siti che mirano ad estorcere le credenziali di accesso dei vari sistemi informatici, qualora vengano inavvertitamente fornite le credenziali a seguito di ricezione di mail appartenenti a tale tipologia, effettuare tempestivamente il cambio della password al fine di impedirne l'illecito utilizzo;
- 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 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, e istituzionali;
- la casella di posta deve essere mantenuta in ordine e in grado di ricevere quotidianamente la posta.

Art. 4 - Misure di sicurezza predisposte dall'Istituzione Scolastica

In ottemperanza al provvedimento del Garante della Privacy del 01/03/2007, l'Istituzione scolastica ha provveduto ad adottare le seguenti misure organizzative finalizzate alla prevenzione di utilizzi non pertinenti e al fine di ridurre il rischio di usi impropri della rete internet:

- individuazione e blocco di categorie di siti internet aventi contenuti e/o finalità estranei all'attività lavorativa scolastica;
- liste di siti bloccati (cd. black list) periodicamente aggiornate di siti internet aventi contenuti e/o finalità vietate dalla legge;
- configurazione di sistemi e utilizzo di filtri (firewall) che prevengono determinate operazioni non correlate all'attività lavorativa;
- blocco di download di file o software aventi particolari caratteristiche dimensionali o di tipologia di dato;
- conservazione nel tempo dei dati strettamente limitata al perseguimento di finalità organizzative, produttive e di sicurezza.

Inoltre il sistema di autorizzazione delle credenziali prevede:

- criteri di individuazione preventiva,
- verifiche periodiche effettuate dall'Amministratore di Sistema sul corretto funzionamento,
- criteri di revoca.

Altre misure di sicurezza adottate sono:

- aggiornamento e verifiche periodiche dell'ambito del trattamento consentito agli incaricati,
- installazione e aggiornamento di software antivirus e per la prevenzione della vulnerabilità,
- back-up regolare e giornaliero dei dati.

Fermo restando che l'utilizzo di Internet nelle numerose funzionalità è consentito esclusivamente in relazione a finalità istituzionali connesse all'attività lavorativa e per gli scopi attinenti alle proprie mansioni, per non limitare le attività tipicamente istituzionali è consentito l'utilizzo di adeguati strumenti di filtraggio e controllo, mediante i quali può essere bloccata la navigazione su categorie di siti i cui contenuti sono stati classificati come certamente estranei agli interessi ed alle attività lavorative.

Art. 5 - Controlli previsti e sanzioni

Qualora le misure tecniche preventive non fossero sufficienti ad evitare eventi dannosi o situazioni di pericolo, l'I.I.S.S. "M.Curie" si riserva di effettuare, in aderenza ai principi di pertinenza e non eccedenza, verifiche di eventuali situazioni anomale.

Nel rispetto della normativa vigente richiamata nelle premesse del presente disciplinare, l'istituzione scolastica non procede a verifiche che possano configurare il controllo a distanza dell'attività dei lavoratori.

L'accesso alle postazioni di lavoro, effettuato tramite le credenziali, viene tracciato secondo le seguenti modalità: tutte le operazioni effettuate, ivi compresi gli accessi, vengono registrate dalle apposite funzioni del server. Tutte le operazioni effettuate, ivi compresi gli accessi, tramite gli applicativi software, vengono registrate dagli applicativi stessi e, come nel caso dei "registri on line" o applicazioni acquisite da "software house" esterne, dalle società terze nominate responsabili.

L'Amministrazione, nella persona del Dirigente Scolastico, si riserva la facoltà di eseguire controlli in conformità alla legge, sia per eseguire verifiche sulla funzionalità e sicurezza di reti e sistemi, sia per eseguire verifiche sul corretto utilizzo dei servizi Internet e posta elettronica, in conformità a quanto prescritto dal presente disciplinare e dalla normativa posta a protezione dei dati personali.

I controlli sono posti in essere dal Titolare del trattamento dati coadiuvato dall'amministratore di sistema. L'istituzione scolastica si potrà avvalere di personale esterno, appositamente nominato quale responsabile esterno di trattamento dei dati e/o amministratore di sistema informatico, secondo le previsioni del D. Lgs. 196/2003.

L'Istituto Scolastico garantisce che il trattamento dei dati personali del personale, effettuato per verificare il corretto utilizzo dei PC interni , della Posta elettronica e di Internet, è conforme ai seguenti principi:

a) ***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);

b) ***il principio di correttezza***, secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note (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;

c) ***principio di pertinenza e non eccedenza*** in virtù del quale:
- i trattamenti devono essere effettuati per finalità determinate, esplicite e legittime ,
- il datore di lavoro deve trattare i dati "*nella misura meno invasiva possibile*",
- le attività di monitoraggio devono essere svolte solo da soggetti preposti e regolarmente incaricati (Amministratore di sistema, tecnici fiduciari, ecc.) ed essere "*mirate sull'area di rischio, tenendo conto della normativa sulla protezione dei dati e, se pertinente, del principio di segretezza della corrispondenza*".

I controlli sono eseguiti tenendo conto del principio di graduazione (par. 6.1 del Provvedimento del Garante per la Protezione dei Dati Personali 1/3/2007) e procederanno come segue:

a) al verificarsi di comportamenti anomali sull'utilizzo degli strumenti informatici che possano prefigurare attività non conformi al presente regolamento, il dirigente scolastico deve effettuare un controllo anonimo su dati aggregati, riferito all'intera struttura amministrativa, oppure a sue aree.

Il controllo anonimo potrà concludersi con un avviso generalizzato relativo all'utilizzo anomalo degli strumenti dell'amministrazione e con l'invito ad attenersi scrupolosamente ai compiti assegnati ed alle istruzioni impartite ai dipendenti; tale avviso potrà essere circoscritto anche solo a dipendenti appartenenti a una certa area in cui si è verificata l'anomalia.

Come comportamenti anomali si intendono, a titolo esemplificativo, l'utilizzo di siti che possono, attraverso anche le funzioni di download, provocare danni alla funzionalità dei sistemi informatici della scuola e alla formazione e conservazione degli archivi e che potrebbero comportare la perdita di dati, il massiccio utilizzo di siti non relativi alla attività di servizio, o, in generale, ad azioni che si possano configurare quali attività non conformi al presente regolamento.

b) in assenza di successive anomalie non si effettueranno controlli su base individuale;

c) nel perdurare delle anomalie si procederà a controlli su base individuale o per postazioni di lavoro;

d) in caso di abusi singoli e reiterati si procederà all'invio di avvisi individuali e si eseguiranno controlli nominativi o su singoli dispositivi e/o postazioni di lavoro;

e) in caso di riscontrato e reiterato uso non conforme delle risorse informatiche, a seguito di ripetute e significative anomalie, rilevate, ad esempio, per la presenza di virus provenienti da siti non istituzionali, l'Amministrazione scolastica potrà svolgere verifiche ex post sui dati inerenti l'accesso alla rete dei dipendenti, e, qualora emergano precise responsabilità del singolo dipendente, il Dirigente Scolastico, effettuate le dovute verifiche del caso, procederà ad avviare il procedimento disciplinare nelle forme e con le modalità di cui al D.lgs. n. 165 del 2001 articoli 55 bis e seguenti.
Resta fermo che, in caso di riscontro di evidenze o fatti penalmente rilevanti, si procederà ad effettuare immediata denuncia alle autorità di pubblica sicurezza e/o giudiziarie.

IL DIRIGENTE SCOLASTICO
Prof. Carmelo Sergi

Allegati:

- Provvedimento del Garante per la Protezione dei Dati Personali 1 marzo 2007 n. 13;
- Informativa ai sensi dell'art. 13 del D.Lgs.n.196/2003 "Codice della privacy", Regolamento Decreto M.P.I. n. 305 del 07/12/2006 e del D.Lgs.n.33/2013, nonché informativa inerente il trattamento dei dati nell'ambito dell'applicativo del registro on line;
- Lettera di nomina del personale docente ad incaricati ai sensi del D.Lgs. n.196/2003 in merito al trattamento dei dati personali e all'utilizzo dei dati nell'ambito dell'applicativo del "Registro on-line".

Il presente Regolamento è stato portato a conoscenza del Consiglio di Istituto
nella seduta del 29/10/2014.
Esso è pubblicato sul sito www.mcurie.gov.it nella sezione Regolamenti di Istituto.