POLICY INFORMATICA

Data: 20/10/2016 Pagine: 32

	Ruolo	Nome	Firma	Data
AUTORE	Amministratore di Sistema	Biagio Tufo		20/10/16
VERIFICATO E APPROVATO	DSGA	Anna Panunzio		20/10/16
EMESSO	DSGA	Anna Panunzio		20/10/16

REVISIONI

Rev.	Data	Autore	Descrizione
1.0	20/10/16	Biagio Tufo	Prima emissione

INDICE

- **INTRODUZIONE** **4**
- **OBIETTIVO** **7**
- **DEFINIZIONE** **8**
  - SISTEMA ICT 8
  - STRUMENTI ICT 8
  - SICUREZZA ICT E RELATIVI RISCHI 8
- **PRINCIPI GENERALI** **9**
- **RUOLI E RESPONSABILITA'** **10**
  - A. AMMINISTRATORE DI SISTEMA 11
  - B. LE RESPONSABILITÀ INDICATE NELLE DISPOSIZIONI CHE SEGUONO SI APPLICANO NELLO STESSO MODO A TUTTI GLI UTENTI 12
- **DISPOSIZIONI** **12**
- **ACCESSO ED USO DEI SISTEMI** **14**
- **INSTALLAZIONE PROGRAMMI** **16**
- **UTILIZZO SUPPORTI MAGNETICI E DATI** **16**
- **UTILIZZO RETE INTERNA (INTRANET DELL'ISTITUTO)** **17**
- **UTILIZZO RETE ESTERNA (INTERNET)** **18**
- **UTILIZZO POSTA ELETTRONICA** **19**
- **PROTEZIONE DEI COMPUTER PORTATILI** **21**
- **PERSONAL COMPUTER NON COLLEGATI ALLA RETE DELL'ISTITUTO** **23**
- **CUSTODIA, CONSERVAZIONE E CONTROLLO DOCUMENTI CARTACEI** **24**
- **GESTIONE DEI DATI INFORMATICI** **24**
- **ATTIVITA' DI VERIFICA** **24**
  - POSTA ELETTRONICA 25
  - RETE ESTERNA (INTERNET) 25
  - RETE INTERNA (INTRANET) 25
- **APPLICAZIONE ED INTERPRETAZIONE** **26**
- **DISCIPLINA DEROGHE E MODIFICHE** **26**
- **RESPONSABILITA'** **27**

REGOLAMENTO INFORMATICO INTERNO

1 INTRODUZIONE

Premesso che:

a) L' I.P.S.E.O.A. Marco Polo pone a disposizione dei dipendenti le risorse informatiche idonee all'espletamento delle singole mansioni;
b) tali risorse informatiche sono di proprietà dell'I.P.S.E.O.A. Marco Polo e pertanto lo stesso è responsabile dell'idoneo utilizzo;
c) l'utilizzo delle risorse informatiche e telematiche dell'Istituto deve sempre ispirarsi ai principi di diligenza e correttezza, atteggiamenti questi destinati a sorreggere ogni atto o comportamento posto in essere nell'ambito del rapporto di lavoro;
d) un utilizzo conforme alla previsioni dell'Istituto consente di evitare rischi e vulnerabilità del sistema informatico;
e) la progressiva diffusione di nuove tecnologie informatiche espone l' I.P.S.E.O.A. Marco Polo a rischi di coinvolgimento sia patrimoniale sia penale creando al contempo problemi di immagine e di sicurezza.
f) in data 1 marzo 2007 l'Autorità Garante per la protezione dei dati personali, ha emanato le linee guida in materia di utilizzo di posta elettronica e di internet nel rapporto di lavoro, indicando ai datori di lavoro l'adozione e la pubblicizzazione di un disciplinare interno in materia di utilizzo delle risorse informatiche;

g) con la pubblicazione nel numero 221 della Gazzetta Ufficiale del 23 settembre 2015 (Suppl. Ordinario n. 53), è entrato in vigore il Decreto Legislativo n. 151 del 14 settembre 2015, recante «Disposizioni di razionalizzazione e semplificazione delle procedure e degli adempimenti a carico di cittadini e imprese e altre disposizioni in materia di rapporto di lavoro e pari opportunità, in attuazione della legge 10 dicembre 2014 n. 183». L'articolo 23 del D.Lgs. n. 151/2015 modifica l'articolo 4 della Legge n. 300 del 1970 – anche nota come Statuto dei Lavoratori – e rimodula il divieto dei controlli a distanza, nella consapevolezza di dover tener conto, nell'attuale contesto produttivo, oltre agli impianti audiovisivi, anche degli altri strumenti «dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori» e di quelli «utilizzati dal lavoratore per rendere la prestazione lavorativa». Pertanto il datore di lavoro secondo la vigente normativa può riservarsi di verificare (direttamente o attraverso la propria struttura) il corretto utilizzo degli strumenti di lavoro, in quanto può raccogliere informazioni mediante gli stessi strumenti di lavoro (pc, notebook, tablet, cellulare) messi a disposizione dei dipendenti o tramite sistemi di registrazione degli accessi e delle presenze, **senza dover stipulare un accordo sindacale** o autorizzazione amministrativa. Per gli *impianti* di sorveglianza fissi (es. videosorveglianza), continua invece ad essere necessario un accordo sindacale o l'autorizzazione della Direzione Territoriale del Lavoro e rimangono ammissibili per esigenze organizzative e produttive, per la sicurezza del lavoro, per la tutela del patrimonio dell'Istituto.

   Le informazioni *raccolte, con entrambe le modalità di cui sopra, possono essere utilizzabili dall' I.P.S.E.O.A. Marco Polo, "per le sole finalità connesse al rapporto di lavoro" quindi senza escludere l'impiego anche per fini disciplinari.*

h) è opportuno diffondere un regolamento informatico in grado di fornire informazioni ed orientamenti ai dipendenti in merito all'utilizzo idoneo della strumentazione.

Il presente regolamento è stato redatto tenendo conto delle previsioni contenute nel:

- **Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali";**
- **Legge 20 maggio 1970 (Statuto dei Lavoratori);**
- **Legge 18 marzo 2008, n. 48 "Delitti informatici e trattamento illecito dei Dati" (Articoli 615 ter, 615 quater, 615 quinquies, 617 quater, 617 quinquies, 635 bis, 635 ter, 635 quater, 635 quinquies, 491 bis e 640 quinquies del Codice Penale);**
- **Modello di Organizzazione, Gestione e Controllo ex Decreto Legislativo 8 giugno 2001 n. 231:**
- **Decreto Legislativo n. 151 del 14 settembre 2015**

Ai sensi del Decreto Legislativo n. 196 del 2003, i dati possono essere classificati come seguono:

- **Personali**: ovvero qualsiasi informazione che riguardi persone, società, enti, associazioni identificati o che possano essere identificati anche attraverso altre informazioni quali, ad esempio, un numero o un codice identificativo.

  Sono dati personali: nome e cognome o denominazione; indirizzo o sede; codice fiscale o partita Iva e qualsiasi ripresa audiovisiva.
- **Sensibili**: dati personali che, per la propria delicatezza, richiedono particolari cautele; essi sono quei dati idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di 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 rivelare lo stato di salute e la vita sessuale.

  Giudiziari: dati personali idonei a rilevare provvedimenti emessi dalle Autorità Giudiziarie e contenuti nel casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reati e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli artt. 60 e 61 c.p.p..

Ai sensi del Decreto Legislativo n. 196 del 2003 le informazioni dell'Istituto possono essere classificate come segue:

- ✓ ***Pubblica***: informazione generale esplicitamente rivolta anche a comunicazione o diffusione indifferenziata all'esterno dell'Istituto.
- ✓ ***Comune***: informazione generale che quindi è da ritenersi riservata dell'Istituto; può essere conosciuta anche da soggetti esterni purché indicati esplicitamente tra i destinatari.
- ✓ ***Riservata:*** informazione rivolta a specifici soggetti destinatari.

ciò premesso, occorre che ciascun dipendente si uniformi al rispetto delle successive regole ed alle indicazioni in materia di utilizzo delle risorse informatiche poste a disposizione, nel rispetto delle disposizioni legislative.

2 OBIETTIVO

Il presente regolamento indica l'ambito di applicazione, principi generali, ruoli e responsabilità per la tutela:

- o delle risorse di Information Communication Technology (ICT) dell'I.P.S.E.O.A. Marco Polo (di seguito Istituto);
- o delle informazioni trattate e gestite tramite le citate risorse.

Il presente regolamento, definisce, inoltre, le attività relative alla sicurezza nell'utilizzo del Sistema ICT ed indica altresì la natura delle verifiche, effettuate dall'Istituto.

1. I sistemi Informatici, le applicazioni, le procedure informatiche, i telefoni cellulari (utilizzati anche come supporti informatici). I software per qualsiasi dispositivo elettronico (computer, palmare, tablet, etc.). I telefoni fissi e cellulari.
2. I componenti dei computer compresi gli accessori interni ed esterni (es. modem, schede di rete, chip di memoria, cavi, memorie di massa etc.)
3. Il cablaggio usato per trasportare informazioni elettroniche (vocali e/o dati);
4. qualsiasi dispositivo di dati;

- **STRUMENTI ICT**

  - Ciascun componente costituente il Sistema ICT;

- **SICUREZZA ICT E RELATIVI RISCHI**

  - Tutte le azioni poste in essere a tutela del patrimonio informativo dell'Istituto contro rischi e/o violazioni che ne possano pregiudicare confidenzialità, integralità, disponibilità ed utilizzabilità, nonché, per estensione, l'insieme di comportamenti, norme, attività e strumenti volti a garantire tale tutela.

3 PRINCIPI GENERALI

Al fine di evitare eventuali **Rischi di Sicurezza** (intendendosi rischio il prodotto tra la probabilità di accadimento di un incidente di Sicurezza e l'intensità del danno diretto o indiretto sul patrimonio dell'Istituto) per l'Istituto, nell'ambito dell'utilizzo e tutela del Sistema ICT è necessario pianificare e porre in essere adeguate misure di carattere tecnologico e organizzativo.
Tali misure devono prevenire possibili azioni dannose (o quanto meno minimizzarne gli effetti), tenendo presente il principio che la sicurezza è un' esigenza dell'Istituto che comporta aspetti organizzativi, procedurali, tecnici, informatici e logistici.
Le attività di seguito riportate sono volte ad evitare comportamenti, consapevoli o inconsapevoli, capaci di concretizzarsi in eventi dannosi.

A tale proposito:

L'Istituto verifica, nei limiti consentiti dalle norme legali e contrattuali e con modalità diffuse ed uniformi:

- L'integrità del proprio Sistema ICT;
- Il rispetto di quanto previsto nel seguito del presente regolamento.

Si evidenzia che l'Istituto non effettua registrazioni al solo scopo di controllo dell'attività lavorativa del proprio personale, ma principalmente interventi volti a salvaguardare la Sicurezza ICT ed il mantenimento dell'efficienza del Sistema ICT.

Le tecnologie utilizzate a tal fine sono compatibili con quanto disposto dalla normativa vigente in materia.
Gli Strumenti ICT costituiscono un mezzo di lavoro e devono essere utilizzati, di norma, per il perseguimento di fini strettamente connessi agli incarichi lavorativi secondo criteri di massima correttezza e professionalità, coerentemente al tipo di attività svolta ed in linea con le disposizioni normative vigenti.
In ogni caso l'utilizzo degli strumenti ICT non configura una titolarità, da parte dell'utente, delle informazioni trattate mediante tali strumenti a cui l' Istituto si riserva pertanto il diritto di accedere nei limiti consentiti dalle norme legali e contrattuali.
La violazione delle previsioni di cui alla presente procedura potrà comportare l'applicazione delle sanzioni disciplinari contemplate dal Contratto Collettivo Nazionale di Lavoro applicabile, nel rispetto dei principi di gradualità e proporzionalità, nonché delle altre misure di tutela del caso.

4 RUOLI E RESPONSABILITA'

Le responsabilità inerenti alla gestione e utilizzo degli Strumenti ICT comportano diversi aspetti di operatività a seconda che sia attribuita a:

A. Amministratore di sistema;

B. Tutti gli altri utenti dell'Istituto (docenti, collaboratori, personale con contratto di somministrazione, personale di ditte fornitrici presenti in Istituto, consulenti, etc.), comunque, tutti coloro che a qualunque titolo sono abilitati con proprio nome di log-on all'utilizzo del Sistema.

A. AMMINISTRATORE DI SISTEMA

Al fine di consentire il corretto utilizzo degli strumenti ICT e tutelare la sicurezza delle informazioni trattate nel Sistema ICT, eventualmente richiedendo la collaborazione delle opportune Unità Organizzative dell'Istituto ha la responsabilità di:

- limitare l'accesso logico al Sistema ICT esclusivamente a personale autorizzato ed in particolare impedire:
  - a personale non autorizzato l'intrusione, dall'esterno o dall'interno, alla rete informatica e telefonica dell'Istituto;
  - il collegamento alla rete dati o alle postazioni di lavoro di dispositivi di elaborazione o di memorizzazione non autorizzati;
  - alterazione al Sistema ICT ed alle informazioni in esso gestite;

- impedire l'accesso a sistemi non autorizzati;

Inoltre, l'amministratore di sistema, ai fini della disponibilità delle informazioni trattate nel Sistema ICT, dovrà assicurare le seguenti misure tecniche organizzative:

- il salvataggio dei dati trattati attraverso opportune procedure di "back-up" e conservazione degli stessi in luoghi diversi da quelli in cui sono collocati i dispositivi di memorizzazione principali del Sistema ICT.
  Il mantenimento dei dati salvati avviene in luoghi che presentano misure di protezione analoghe a quelle definite dalla normativa attuale per il trattamento degli specifici dati;

- la disponibilità del servizio erogato dal Sistema ICT attraverso:

    - continuità elettrica: attivazione, in caso di interruzione della fornitura di elettricità, di misure atte a garantire il servizio per il tempo necessario ad espletare eventuali attività utente improcrastinabili, limitatamente alle attrezzature ed ai componenti del Sistema ICT individuati dall'Istituto come critici;

    - continuità operativa: definizione ed attuazione di un piano di Disaster Recovery che consenta, dopo un'interruzione del servizio, il ripristino dell'operatività del Sistema ICT per quei processi e attività individuati dall'Istituto come critici.

B. LE RESPONSABILITÀ INDICATE NELLE DISPOSIZIONI CHE SEGUONO SI APPLICANO NELLO STESSO MODO A TUTTI GLI UTENTI

5 DISPOSIZIONI

Utilizzo della strumentazione:

1. E' fatto divieto installare sulla strumentazione in uso, hardware fisso o removibile (ad esempio modem) qualora ciò non risulti espressamente richiesto ed autorizzato dall'Istituto.
2. L' Istituto si riserva di rimuovere qualsiasi elemento hardware la cui installazione non sia stata appositamente prevista e autorizzata.
3. L'amministratore di sistema provvederà a pre-impostare le singole postazioni affinché trascorsi 10 minuti di inattività, si attivi automaticamente il salva-schermo protetto da password;

è onere/dovere del dipendente non alterare alcuna impostazione di Sicurezza e segnalare, qualora la misura di protezione non sia attiva sul proprio pc, tale anomalia ai Sistemi Informativi i quali provvederanno al suo ripristino.

4. Sui PC dotati di scheda audio e/o di lettore CD non è consentito l'ascolto di programmi, file audio o musicali, se non a fini prettamente lavorativi.
5. Qualora si rendessero necessarie modifiche alle configurazioni impostate sul PC in uso, occorre farne richiesta ai Sistemi Informativi.
6. Si ricorda al dipendente che è suo dovere conservare la strumentazione informatica in buono stato, segnalare prontamente guasti o anomalie che possano pregiudicarne il funzionamento e di spegnere il PC in uso al termine della giornata di lavoro. Inoltre rammentiamo il divieto di pubblicare su siti o portali online, foto e/o video ripresi all'interno dell'Istituto.
7. Qualora il dipendente disponesse di risorse informatiche non più necessarie per la propria postazione, deve darne avviso all'amministratore di sistema affinché le risorse siano riassegnate ad altre postazioni.
8. Qualsiasi spostamento della strumentazione ICT all'interno dell'Istituto deve essere preventivamente autorizzato dall'amministratore di sistema.

9. **E' inoltre assolutamente <u>vietato</u> utilizzare in Istituto strumenti ICT personali (PC, periferiche, dispositivi di memorizzazione, tablet, etc.) se non preventivamente autorizzati dal titolare dell'Istituto.**

6 ACCESSO ED USO DEI SISTEMI

1. Qualsiasi creazione o modifica di Account informatici dovrà essere richiesta al responsabile dell'Istituto. Tale richiesta darà l'avvio ad un iter autorizzativo che coinvolgerà sia il responsabile dell'Istituto che l'amministratore di sistema.
2. Le unità disco (locali o di rete) sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi.
   Pertanto qualunque file che non sia connesso all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità.
3. Il dipendente si connette alla rete tramite autenticazione univoca personale, che gestisce in autonomia e con piena responsabilità delle proprie password. In nessun caso devono essere annotate password in chiaro sia su supporto cartaceo (es. post it) che informatico (es. fogli excel, word, notepad, etc.).
4. I requisiti minimi di complessità delle password come espressamente richieste dal legislatore sono:

- redazione con caratteri maiuscoli e/o minuscoli;
- possibilità di includere simboli, numeri, punteggiatura e lettere;
- utilizzo di almeno 8 caratteri nella composizione della password (sono esclusi da tale obbligo i sistemi operativi che non supportano tali requisiti);

- divieto di composizione di password basate su informazioni personali, riferimenti familiari o comunque dati inerenti direttamente il soggetto titolare della password stessa (a titolo meramente esemplificativo: evitare di utilizzare nominativi personali o familiari, date di nascita, codici fiscali o comunque informazioni personali facilmente rintracciabili).

5. Il dipendente titolare della password è tenuto a non rivelare ad alcuno la password dovendone avere la massima diligenza e preservandone la segretezza anche durante il momento della digitazione.
6. Qualora il dipendente ritenga che un soggetto non autorizzato può aver visionato la digitazione o essere comunque a conoscenza della password, deve immediatamente cambiarla.
7. Qualora al dipendente sia richiesto di riferire in qualunque forma la password (telefonicamente, via e-mail, localmente) il dipendente è obbligato a rifiutarsi; contemporaneamente deve dare immediata comunicazione dell'accaduto al titolare dell'Istituto.
8. Per motivi di sicurezza, quando si accede a caselle di web-mail dell'Istituto, è fatto divieto di salvare la password di accesso utilizzando le opzioni di compilazione automatica di cui sono dotati i browser.
9. Al dipendente sarà richiesto con cadenza trimestrale, di reinserire una nuova password.
10. Ciascun dipendente deve fare un uso conforme dei dati secondo le credenziali di autenticazione fornitegli per i vari livello di accesso. La conoscenza di particolari modalità di accesso che vadano oltre quanto consentito al dipendente secondo il proprio ruolo, non deve mai giustificare una consultazione di dati diversa rispetto a quella originariamente stabilita dall'Istituto.

7 INSTALLAZIONE PROGRAMMI

1. Sul pc in uso, **è assolutamente vietato** installare programmi che non siano ufficialmente forniti dall'Istituto per il tramite dei soggetti appositamente incaricati all'installazione.

2. L'Istituto ricorda al dipendente che costituiscono illecito penale le condotte consistenti nella illecita duplicazione o riproduzione di software e file multimediali ai sensi della legge sul diritto d'autore n. 633/41.

3. Per qualunque tipo di modifica al sistema informatico il dipendente è tenuto a presentare opportuna richiesta di assistenza all'amministratore di sistema, la richiesta sarà analizzata dallo stesso amministratore che procederà, qualora la richiesta sia stata autorizzata dal titolare dell'Istituto, ad apportare la modifica richiesta.

L'amministratore di sistema è autorizzato a provvedere a tali variazioni solo e soltanto in presenza di una richiesta scritta di Assistenza.

8 UTILIZZO SUPPORTI MAGNETICI E DATI

1. È fatto obbligo al dipendente conservare, custodire e controllare i supporti informatici removibili contenenti dati, informazioni, notizie anche in forma cartacea o immagini di attinenza dell'Istituto, affinché nessun soggetto terzo ne prenda visione o possesso.

2. Il dipendente non deve creare/scaricare/salvare file estranei all'attività lavorativa, sul pc in uso.

3. Qualora il dipendente abbia incertezze sulla provenienza di un file, deve prontamente rivolgersi all'amministratore di sistema il quale effettuerà le opportune verifiche sulla sussistenza di eventuali rischi di sicurezza connessi a quel file.

9 UTILIZZO RETE INTERNA (INTRANET DELL'ISTITUTO

1. La rete interna, istituita appositamente per permettere collegamenti funzionali tra i dipendenti, non può esser utilizzata per scopi diversi da quelli di tipo dell'Istituto.
2. Qualora nella rete interna debbano circolare dati, notizie ed informazioni dell'Istituto, deve essere premura di ciascun dipendente preservare gli stessi dalla conoscibilità di terzi soggetti non espressamente autorizzati ad aver notizia di tali dati.

E' assolutamente vietata l'introduzione di dati e/o documenti classificati in rete.

3. Si comunica che qualora il dipendente non si autentichi alla rete dell'Istituto per un periodo superiore a 20 giorni consecutivi, l'amministratore di sistema ne darà comunicazione al titolare dell'Istituto al fine di verificare eventuali disattivazioni delle credenziali assegnate.
4. **E' assolutamente vietato:**

- falsificare documenti informatici pubblici o privati aventi efficacia probatoria (art. 491 bis c.p.);
- accedere abusivamente ad un sistema informatico o telematico (art. 615 ter c.p.);
- detenere o diffondere abusivamente codici di accesso a sistemi informatici o telematici (art. 615 quater c.p.);
- diffondere programmi diretti o danneggiare o interrompere un servizio telematico (art. 615 quinquies);
- intercettare, impedire o interrompere illecitamente comunicazioni informatiche o telematiche (art. 617 quater c.p.);

♐☜ installare apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche (art. 617 quinquies);

♑☜ danneggiare informazioni dati e programmi informatici privati o utilizzati dallo Stato o da altro Ente Pubblico o di pubblica utilità (art. 635 bis e art. 635 ter c.p.);

♒☜ danneggiare sistemi informatici o telematici privati di pubblica utilità (art.635 quater e art. 635 uinquies c.p.);

♓☜ violare, da parte del soggetto che presta servizi di certificazione di firma elettronica, gli obblighi previsti dalla Legge per il rilascio di un certificato qualificato (art. 640 quinquies c.p.).

10 UTILIZZO RETE ESTERNA (INTERNET)

Gli utenti ai quali è accordato l'accesso ad internet, vengono individuati dall'Istituto, e relativa necessità segnalata all'amministratore di sistema.

L'utente deve accedere ad Internet allo scopo di svolgere le attività correlate al proprio lavoro, e comunque per gli usi indicati e nel rispetto delle regole di seguito descritte.

1. E' assolutamente vietato scaricare/salvare dalla rete Internet documenti, file o dati comunque non attinenti le mansioni assegnate al singolo dipendente. In particolare è vietato:

   a) navigare in siti non attinenti allo svolgimento delle mansioni assegnate e su *social network (es. Facebook, Twitter, etc.)*;
   b) effettuare transazioni finanziaria ivi comprese le operazioni di *remote banking,* acquisti *on-line* e simili;
   c) scaricare software di ogni e qualsivoglia natura;
   d) effettuare registrazioni a siti i cui contenuti non siano legati all'attività lavorativa;

e) partecipare, per motivi non professionali, a *Forum*, l'utilizzo di *chat on line* , di bacheche elettroniche e le registrazioni in *guest book* anche utilizzando pseudonimi (o *nicknames*).

2. Qualsiasi dato non attinente all'attività lavorativa rilevato sui pc in uso agli utenti, sarà cancellato.

11 UTILIZZO POSTA ELETTRONICA

1. Le caselle di posta elettronica date in uso al dipendente sono destinate ad un utilizzo tassativamente ed esclusivamente inerente l'attività lavorativa. Si precisa che:

a) è assolutamente vietato inviare o memorizzare messaggi di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;

b) è assolutamente vietato l'utilizzo dell'indirizzo di posta elettronica dell'Istituto per la partecipazione a dibattiti, *Forum, newsletter* o *mail-list,* non attinenti la propria mansione.

c) è assolutamente vietato lo scambio di messaggi sotto mentite spoglie, ossia impersonando un mittente diverso da quello reale, in quanto comportamento illecito;

d) è assolutamente vietato inviare messaggi di posta (con o senza allegato) contenenti:

- **dati riservati dell'Istituto (company confidential) o classificati;**
- immagini, filmati, e qualunque tipo di file dai contenuti illegali, violenti e/o pornografici;
- file soggetti a diritto d'autore (file musicali, video o eseguibili di programma, ad es.:mp3, divx,avi,exe etc.);
- link a siti con contenuti illegali, violenti e/o pornografici;
- password e/o codici di accesso a programmi soggetti a diritto d'autore.

Non è consentito aprire messaggi di posta con allegati contenenti file "eseguibili", salvo caso di certezza assoluta del mittente.

Per quanto riguarda l'origine dei messaggi di posta, si deve considerare che è facile impersonare un mittente diverso da quello reale, soprattutto per i generatori di messaggi malevoli;

e) è assolutamente vietato rispondere a messaggi di posta elettronica che:
   - contengono un messaggio generico di richiesta informazioni personali per motivi non ben specificati (ad. es. scadenza, smarrimento, problemi tecnici);
   - fanno uso di toni "intidiminatori", quali ad esempio la minaccia del blocco della carta di credito o del conto corrente in caso di mancata risposta dell'utente.

     Le Banche e gli Istituti di Credito, infatti, non richiedono mai per posta elettronica informazioni attinenti il conto personale o depositi. Le suddette precauzioni hanno lo scopo di evitare che sia "rubata l'identità" e che siano eseguite operazioni ad insaputa dell'utente vittima.

Inoltre, ogni singolo utente ha l'obbligo di:

a) limitare la dimensione del messaggio inviato, soprattutto nei casi in cui vi siano più destinatari. Un allegato di dimensioni eccessive potrebbe impedire l'arrivo del messaggio o richiedere un uso eccessivo delle risorse; a tal fine la dimensione massima consigliata, per gli allegati, non deve superare i 10 Mbyte.
b) Gestire la casella di posta elettronica, la cui dimensione è stabilita in funzione delle necessità operative, in modo opportuno, eliminando i messaggi non necessari, contenendo la dimensione degli stessi e dei relativi allegati. Ciò al fine di conseguire un più efficace impiego del servizio

di posta elettronica e nel contempo non sovraccaricare i relativi sistemi di sicurezza;

2. L' Istituto comunica che, in caso di assenza improvvisa e/o prolungata, ricorrano improrogabili necessità legate all'attività lavorativa per cui si debba conoscere il contenuto dei messaggi di posta elettronica, come indicato dalle Linee guida del Garante per la protezione dei dati personali per l'utilizzo della posta elettronica nel rapporto di lavoro del 1 Marzo 2007, il Responsabile di Funzione/Direzione di appartenenza dell'utente può richiedere al fiduciario del lavoratore (se nominato per iscritto dall'interessato) di verificare il contenuto di messaggi ed a inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa, in caso di assenza di nomina del fiduciario, il Responsabile di Funzione/Direzione può richiedere ai Sistemi Informativi dell'Istituto, nello specifico al Custode delle credenziali, di accedere alla casella di posta dell'utente stesso, tramite l'apertura della busta contenente la password del lavoratore, busta consegnata dallo stesso al Custode delle credenziali.
   In entrambi i casi, di tale attività deve essere redatto, a cura del suddetto Responsabile, apposito verbale e deve essere informato l'utente interessato, preventivamente o, ove ciò non sia possibile, alla prima occasione utile.
3. In caso di **licenziamento o dimissioni o trasferimento** di un dipendente, il titolare del trattamento comunicherà all'amministratore di sistema di chiudere immediatamente l'**email dell'Istituto** del dipendente (es. nome@marcopologenova.net) e di attivare un sistema automatizzato per comunicare ad eventuali terzi la chiusura dell' indirizzo email, segnalando un account dell'Istituto alternativo al contatto utilizzato fino a quel momento.

12 PROTEZIONE DEGLI APPARATI/ELABORATORI PORTATILI

Tutte le indicazioni riportate ai punti precedenti sono adottate anche per i computer portatili, per tutti gli elaboratori portatili (palmari, tablet, blackberry, etc) e per gli smartphone per i quali è tuttavia necessario aggiungere ulteriori precauzioni, ponendo particolare attenzione nel caso di utilizzo dell'apparato in ambito esterno all'Istituto.
In particolare l'utente deve:

a) proteggere l'elaboratore portatile tramite apposito dispositivo di ancoraggio in caso di utilizzo all'interno dell' Istituto;
b) conservare in un luogo sicuro l'elaboratore/apparato portatile (es.: PC, tablet, palmari, smartphone ecc.) a fine giornata lavorativa;
c) custodire l'elaboratore in caso di trasporto e/o utilizzo in ambito esterno all'Istituto;
d) avvertire tempestivamente, in caso di furto di un elaboratore/apparato portatile, il titolare dell'Istituto che darà le opportune indicazioni.

Inoltre, in caso di utilizzo dell'elaboratore in ambito esterno all'Istituto, l'utente deve adottare le misure idonee a garantire la protezione delle informazioni.
A tale scopo l'amministratore di sistema renderà disponibili appositi sistemi di criptatura delle informazioni memorizzate sull'elaboratore e sistemi sicuri di accesso remoto: è responsabilità dell'utente che deve operare in ambito esterno all'Istituto fare richiesta dei necessari strumenti di protezione, previa approvazione del datore di lavoro.

Tutta la gestione degli Strumenti ICT, incluse le modifiche alla configurazione dei sistemi desktop e portatili, deve essere effettuata unicamente dall'amministratore di sistema. Gli utenti non sono autorizzati a modificare il Sistema ICT, neppure se si tratta della postazione di lavoro che hanno ricevuto in assegnazione dall' Istituto.

A titolo esemplificativo, ma non esaustivo, si enunciano attività che sono considerate modifiche del Sistema ICT:

a) spostare o separare i componenti dalla postazione di lavoro;

b) modificare i collegamenti di rete esistenti;

c) usare dispositivi removibili (CD, DVD, Hard Disk, penne USB….) per alterare la procedura di avvio del dispositivo ed in particolare per effettuare l'avvio di un sistema operativo diverso da quello fornito dall' Istituto;

d) aprire la struttura esterna dell'elaboratore e procedere alla modifica (eliminazione o aggiunta) dei componenti dello stesso;

e) installare un qualsiasi software, inclusi quelli scaricati da Internet o comunque alterare la configurazione del PC ricevuta in assegnazione.

E' vietato intervenire sull'hardware per evitare che le garanzie siano violate, anche inavvertitamente, e che le norme di sicurezza siano aggirate.

Si ricorda che l'utilizzo dei notebook all'esterno della rete dell'Istituto non deve in alcun modo alterarne la configurazione software originaria.

13 PERSONAL COMPUTER NON COLLEGATI ALLA RETE DELL'ISTITUTO

E' fatto obbligo al dipendente, di preservare l'integrità del sistema non alterandone in alcun modo le peculiarità soprattutto quando tali pc costituiscono ambienti di sviluppo software.
Inoltre, anche per pc costituenti ambienti di sviluppo, come già riportato per i notebook, è auspicabile l'utilizzo di sistemi di criptatura dati messi a disposizione dai Sistemi Informativi dell'Istituto in quanto in essi possono essere salvati dati sensibili.

14 CUSTODIA, CONSERVAZIONE E CONTROLLO DOCUMENTI CARTACEI

1. E' fatto obbligo al dipendente di custodire il materiale cartaceo derivante da file affinché nessuno ne prenda visione, possa manipolarlo o riprodurlo.

2. **È fatto divieto lasciare qualsiasi documento incustodito presso la propria postazione qualora sia previsto un allontanamento per un lasso di tempo tale da consentirne eventualmente la visione da parte di terzi.**

3. È fatto divieto lasciare qualsiasi documento in locali estranei alla propria postazione, prestando particolare attenzione a non lasciarli presso la fotocopiatrice.

15 GESTIONE DEI DATI INFORMATICI

È fatto divieto applicare sistemi di scrittura segreta o in codice ai dati se non espressamente autorizzati per iscritto dal titolare della Istituto e dall'amministratore di sistema.

16 ATTIVITA' DI VERIFICA

Come sopra evidenziato l' Istituto per prevenire o correggere malfunzionamenti del proprio Sistema ICT nonché garantire l'efficienza dello stesso, effettua registrazioni delle componenti di traffico riferiti a:

- **POSTA ELETTRONICA**

Le informazioni relative ai messaggi di posta elettronica sono analizzate in forma aggregata. Esse vengono mantenute integralmente in linea e sono direttamente consultabili dai soggetti sotto individuati per 30 giorni; oltre tale data le informazioni vengono salvate su un'area di disco e successivamente (periodicamente) vengono memorizzate su supporti ottici non riscrivibili conservati in apposita cassaforte ignifuga. Viene mantenuto lo storico degli ultimi 12 mesi, mentre per i log anteriori si provvede alla distruzione fisica.

Alle informazioni raccolte possano accedere le sole persone, espressamente autorizzate dal titolare della Istituto alla gestione del servizio di Posta Elettronica. ***Le informazioni raccolte, senza che sia necessario un accordo con le rappresentanze sindacali o con la Direzione Territoriale del Lavoro, potranno*** **essere utilizzabili a tutti i fini connessi al rapporto di lavoro,** quindi senza escludere l'impiego anche per fini disciplinari**, come indicato dall' articolo 23 del D.Lgs. n. 151/2015**;

- **RETE ESTERNA (INTERNET)**

Le informazioni relative ai servizi Internet sono raccolte, conservate ed analizzate secondo le modalità sopra descritte per il servizio di Posta Elettronica.

Alle informazioni raccolte possano accedere le sole persone, espressamente autorizzate dal titolare della Istituto alla gestione del servizio Internet;

- **RETE INTERNA (INTRANET)**

Le informazioni relative ai servizi Intranet sono raccolte, conservate ed analizzate secondo le modalità sopra descritte per il servizio di Posta Elettronica.
Alle informazioni raccolte possano accedere le sole persone, espressamente autorizzate dal titolare della Istituto alla gestione del servizio Internet;

- ***Telefonia (fissa e mobile)***

Le informazioni relative ai servizi di telefonia sono raccolte, conservate ed analizzate secondo le modalità sopra descritte per il servizio di Posta Elettronica.
Alle informazioni raccolte possano accedere le sole persone, espressamente autorizzate dal titolare della Istituto alla gestione del servizio di telefonia. ***Le informazioni raccolte, senza che sia necessario un accordo con le rappresentanze sindacali o con la Direzione Territoriale del Lavoro, potranno* essere utilizzabili a tutti i fini connessi al rapporto di lavoro,** quindi senza escludere l'impiego anche per fini disciplinari**, come indicato dall' articolo 23 del D.Lgs. n. 151/2015**

- ***Videosorveglianza***

  Le immagini trasmesse dal sistema di videosorveglianza installato nella sede dell' Istituto non vengono registrate, **le informazioni rilevate potranno essere utilizzabili a tutti i fini connessi al rapporto di lavoro,** quindi senza escludere l'impiego anche per fini disciplinari**, come indicato dall' articolo 23 del D.Lgs. n. 151/2015**

- ***Sistemi di r*****egistrazione degli accessi e delle presenze**

  Le informazioni raccolte, senza che sia necessario un accordo con le rappresentanze sindacali o con la Direzione Territoriale del Lavoro, potranno **essere utilizzabili a tutti i fini connessi al rapporto di lavoro,** quindi senza escludere l'impiego anche per fini disciplinari**, come indicato dall' articolo 23 del D.Lgs. n. 151/2015**

17 APPLICAZIONE ED INTERPRETAZIONE

Per qualsiasi chiarimento relativo all'applicazione pratica o all'interpretazione del presente regolamento, il dipendente può rivolgersi al responsabile dell'Istituto.

18 DISCIPLINA DEROGHE E MODIFICHE

1. Nel caso in cui al presente regolamento l' Istituto intenda apporre modifiche, queste saranno applicate dandone conoscenza immediata al dipendente.

2. Deroghe o modifiche di uno o più punti del presente regolamento, non rendono invalidi gli altri punti. Qualora due o più clausole siano evidentemente incompatibili tra loro, prevarrà la clausola temporalmente più recente.

19 RESPONSABILITA'

1. La violazione di una qualsiasi delle clausole di cui al presente regolamento può generare un richiamo disciplinare del dipendente.
2. Qualora l'Istituto venga a conoscenza di una violazione del presente regolamento che costituisca illecito civile o penale, provvederà immediatamente a darne avviso alla Competente Autorità.
3. Si ricorda che secondo le specifiche previsioni di cui al presente regolamento, l' Istituto verificherà, nei limiti consentiti dalle norme di legge e contrattuali (tramite controlli di tipo "difensivo" che derivano, in specie, dal diritto, riconosciuto al datore di lavoro dall'art. 2104 c.c., di impartire disposizioni per l'esecuzione e la disciplina del lavoro), il rispetto delle regole e l'integrità del proprio sistema informatico.

Per presa visione:

Data	Cognome e Nome	Firma