Prot. n. 8922

Cittadella, 2.10.2018

ALL'ALBO SINDACALE
NEL SITO DELLA SCUOLA
(LEGGI E REGOLAMENTI)

DISCIPLINARE INFORMATICO ISTITUZIONALE
DELL'ISTITUTO IIS A. MEUCCI

INDICE

0. PREMESSA

La progressiva diffusione delle nuove tecnologie informatiche, ed in particolare il libero accesso alla rete Internet dai Personal Computer, espone l'Istituto IIS A. Meucci ai rischi di un coinvolgimento sia patrimoniale sia penale, creando problemi alla sicurezza e all'immagine dell'Istituto stesso.
Premesso quindi che l'utilizzo delle risorse informatiche e telematiche della nostra Istituto deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro, l'Istituto IIS A. Meucci ha adottato un Regolamento interno diretto ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla Sicurezza nel trattamento dei dati.
Il presente regolamento integra le disposizioni di cui agli artt. 2104 e 2105 codice civile, quelle dei CCNL e delle procedure e regolamenti adottati in Istituto e trova applicazione nei confronti dei dipendenti o di altro personale, anche esterno, (da qui in avanti anche detti "utenti") che, in ragione delle mansioni e/o delle attività assegnate e del lavoro e/o della collaborazione da svolgersi, abbiano in dotazione un personal computer, un cellulare o altro dispositivo con connessione a Internet, nonché una casella di posta elettronica Istituzionale.
Le prescrizioni di seguito previste si aggiungono ed integrano, inoltre, le specifiche istruzioni già fornite a tutti gli incaricati in attuazione del GDPR 2016/679 e dalla normativa nazionale vigente contenente le misure di sicurezza.
Considerato inoltre che l'Istituto IIS A. Meucci, nell'ottica di uno svolgimento proficuo e più agevole della propria attività, ha da tempo deciso di mettere a disposizione dei propri dipendenti, che ne necessitassero per il tipo di funzioni svolte, telefoni e mezzi di comunicazione adeguati (computer portatili, telefoni cellulari, tablet, etc.), sono state inserite nel regolamento alcune clausole relative alle modalità ed i doveri che ciascun dipendente deve osservare nell'utilizzo di tale strumentazione. In tal senso si specifica che è consentito un uso personale di questi mezzi fuori dall'orario di lavoro o durante le pause.

1. UTILIZZO DEL PERSONAL COMPUTER

Il Personal Computer e, più in generale qualsiasi strumento e/o mezzo informatico, affidato al dipendente è da considerarsi a tutti gli effetti uno **strumento di lavoro**. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.
L'accesso all'elaboratore è protetto da password che deve essere custodita dall'incaricato con la massima diligenza e non divulgata. La stessa password deve essere attivata per l'accesso alla rete, per lo screen saver e per il collegamento ad Internet. Non è consentita l'attivazione della password di accensione (bios), senza preventiva autorizzazione da parte dell'Incaricato della gestione e manutenzione dei Sistemi Elettronici.

Il custode delle parole chiave riservate**,** per l'espletamento delle sue funzioni, ha la facoltà in qualunque momento di accedere ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica interna ed esterna, secondo quanto previsto al punto 6 del presente regolamento.
Il custode delle parole chiave o un suo incaricato potrà accedere ai dati ed agli strumenti informatici esclusivamente per permettere alla stessa Istituto, titolare del trattamento, di accedere ai dati trattati da ogni incaricato con le modalità fissate dalla stessa Istituto, al solo fine di garantire l'operatività, la sicurezza del sistema ed il normale svolgimento dell'attività dell'Istituto nei casi in cui si renda indispensabile ed indifferibile l'intervento, ad esempio in caso di prolungata assenza od impedimento dell'incaricato, informando tempestivamente l'incaricato dell'intervento di accesso realizzato.
Non è consentito installare autonomamente programmi provenienti dall'esterno salvo previa autorizzazione esplicita dell'Incaricato della gestione e manutenzione dei Sistemi Elettronici, in quanto sussiste il grave pericolo di portare Virus informatici e di alterare la stabilità delle applicazioni dell'elaboratore.
Non è consentito l'uso di programmi diversi da quelli distribuiti ed installati ufficialmente dal responsabile dei sistemi informativi dell'Istituto IIS A. Meucci. L'inosservanza di questa disposizione, infatti, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre l'Istituto a gravi responsabilità civili ed anche penali in caso di violazione della normativa a tutela dei diritti d'autore sul software (D. Lgs. 518/92 sulla tutela giuridica del software e L. 248/2000 nuove norme di tutela del diritto d'autore) che impone la presenza nel sistema di software regolarmente licenziato o comunque libero e quindi non protetto dal diritto d'autore.
Non è consentito all'utente modificare le caratteristiche impostate sul proprio PC, salvo previa autorizzazione esplicita dell'Incaricato della gestione e manutenzione dei Sistemi Elettronici.
Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio. In ogni caso lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso. Eccezione a tale disposizione è rappresentata da una specifica richiesta da arte dell'Incaricato della gestione e manutenzione dei Sistemi Elettronici per motivi di manutenzione e/o implementazione del Sistema Informativo medesimo. In ogni caso deve essere attivato lo screen saver e la relativa password.
Non è consentita l'installazione sul proprio PC di nessun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, chiavette UMTS, etc.), se non con l'autorizzazione espressa dell'Incaricato della gestione e manutenzione dei Sistemi Elettronici.
Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente l'Incaricato della gestione e manutenzione dei Sistemi Elettronici nel caso in cui vengano rilevati virus.
Tutti i PC devono essere dotati di SOFTWARE ANTIVIRUS aggiornato costantemente e con la funzione "Monitor" attiva.

2. UTILIZZO DELLA RETE ISTITUZIONALE

Le unità di rete sono aree di condivisione d'informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità, vengono svolte regolari attività di controllo, amministrazione e backup.
Le password d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite. È assolutamente proibito entrare nella rete e nei programmi con altri nomi utente.
L'Incaricato della gestione e manutenzione dei Sistemi Elettronici può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza sia sui PC degli incaricati sia sulle unità di rete.
Costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. È infatti assolutamente da evitare un'archiviazione ridondante.
È cura dell'utente effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni. È buona regola evitare di stampare documenti o file non adatti (molto lunghi o non supportati) su stampanti comuni. In caso di necessità la stampa in corso può essere cancellata.

3. GESTIONE DELLE PASSWORD

Le password d'ingresso alla rete, di accesso ai programmi e dello screen saver, sono previste ed attribuite dall'Incaricato della gestione e manutenzione dei Sistemi Elettronici. E' necessario procedere alla modifica della password a cura dell'incaricato del trattamento al primo utilizzo e, successivamente, almeno ogni sei mesi; nel caso di trattamento di dati sensibili e di dati giudiziari la periodicità della variazione deve essere ridotta a tre mesi con contestuale comunicazione al Custode delle Parole chiave.
Le password possono essere formate da lettere (maiuscole o minuscole) e numeri ricordando che lettere maiuscole e minuscole hanno significati diversi per il sistema; devono essere composte da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'incaricato (punto 5 del disciplinare tecnico. E' vietato l'uso del proprio nome e/o cognome, di quello dei propri familiari, del proprio luogo e della propria data di nascita e, in generale, di qualsiasi altro riferimento anagrafico).

La password deve essere immediatamente sostituita, dandone comunicazione al Custode delle Parole chiave, nel caso si sospetti che la stessa abbia perso la segretezza.
Qualora l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia alla Direzione o al Delegato Privacy.

4. UTILIZZO DEI SUPPORTI MAGNETICI

Nel caso in cui siano utilizzati supporti informatici quali floppy disk, chiavette usb, schede SSD, cd-rom o nastri per la memorizzazione di dati personali particolari, gli Incaricati devono osservare alcune misure di sicurezza al fine di salvaguardare la riservatezza dei dati:

- i supporti informatici già contenenti dati personali particolari possono essere riutilizzati solo dopo aver provveduto a cancellare i dati e le informazioni in essi contenuti, in modo che non siano tecnicamente ed in alcun modo recuperabili;
- qualora si riscontrassero delle difficoltà nello svolgimento di tali operazioni, si può richiedere l'intervento dell'incaricato della gestione e manutenzione dei Sistemi Elettronici;
- qualora la procedura di cancellazione dei dati risulti inapplicabile, al termine delle operazioni di trattamento i supporti di memoria utilizzati devono essere distrutti;
- fra i supporti di memorizzazione sono ricompresi a pieno titolo i dischi equipaggiati nei computer dimessi e/o sostituiti dai dipendenti.
- l'Istituto IIS A. Meucci non risponderà della perdita dei dati strettamente personali, eventualmente archiviati nella propria postazione di lavoro, il cui trattamento in ogni caso non deve interferire con la normale attività lavorativa. In particolare tali dati non potranno essere salvati nei server Istituzionali.

L'incaricato del trattamento dei dati ha la responsabilità di:

- segnalare la necessità di un'eventuale riparazione degli hard disk;
- segnalare la necessità di un'eventuale dismissione dei CD-ROM, dei nastri magnetici, dei floppy disk, delle chiavette usb e delle schede SSD;
- segnalare la necessità di un'eventuale dismissione dei floppy disk; degli hard disk, dei nastri magnetici, delle chiavette usb e delle schede SSD;
- eseguire la re-inizializzazione dei floppy disk, delle chiavette usb e delle schede SSD per poterli successivamente riutilizzare;
- effettuare il test sulla re-inizializzazione dei floppy disk, delle chiavette usb e delle schede SSD eseguita precedentemente.

Le attività d'uso e riuso sono possibili solo se disposte ed autorizzate specificatamente dal proprio responsabile e ogni caso non devono in alcun modo pregiudicare I livelli di sicurezza richiesti dall'attività specifica dell'Istituto IIS A. Meucci.
I supporti magnetici contenenti dati sensibili e giudiziari (punto 21 del disciplinare tecnico) devono essere custoditi in archivi chiusi a chiave.

5. UTILIZZO DI PC PORTATILI

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

6. USO DELLA POSTA ELETTRONICA

Il dipendente può accedere alla sua casella di posta elettronica da tutti gli strumenti che utilizza (*Desktop*, *Laptop*, *Tablet*, Telefono Mobile). Gli strumenti dovranno essere dotati dei requisiti di sicurezza definiti dal presente documento; l'Area ICT può richiedere l'eventuale installazione di appositi applicativi di sicurezza
E' onere dell'utente procedere all'invio alla Segreteria, di tutti i messaggi ricevuti che hanno carattere lavorativo e per i quali è prevista dalle procedure Istituzionali una specifica protocollazione.
Nell'utilizzo del servizio ciascun utente è tenuto a attivare, in caso di assenza prolungata, la funzione di risposta automatica che inviti il mittente a prendere contatto con altre risorse dell'Istituto.
La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e allegati ingombranti.
l messaggi inviati o ricevuti dall'Utente sono raccolti sul server di posta elettronica Istituzionale, in cui rimangono conservati in base allo spazio di memoria disponibile per la casella assegnata a ciascun utente, secondo le prassi Istituzionali. Tali messaggi sono archiviati automaticamente su sistemi di archiviazione Istituzionale.
I contenuti delle singole caselle di posta elettronica sono soggetti a periodico backup.
Le informazioni contenute nei messaggi di posta elettronica sono da considerarsi riservate e confidenziali.
Il loro utilizzo è consentito esclusivamente al destinatario in indirizzo e ne è vietata la diffusione in qualunque modo

eseguita, salvo che ne sia data espressa autorizzazione da parte del mittente.
È fatto divieto di utilizzare le caselle di posta elettronica *nome.cognome@meuccifanoli.gov.it* per motivi diversi da quelli strettamente legati all'attività lavorativa. In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare la posta elettronica Istituzionale per:

- trasmettere a soggetti esterni a l'Istituto IIS A. Meucci informazioni riservate o comunque documenti Istituzionali, se non nel caso in cui ciò sia necessario in ragione delle mansioni svolte, per l'adempimento di un obbligo di legge o di contratto di cui sia parte l'Istituto IIS A. Meucci o al fine di difendere un diritto dell'Istituto IIS A. Meucci;
- di messaggi aventi contenuto lesivo per la reputazione dell'Istituto e che gettino discredito sulla medesima o il compimento di qualsiasi atto o fatto illecito attraverso l'utilizzo della casella Istituzionale che possano far attribuire all'Istituto IIS A. Meucci ed a chi la rappresenta una responsabilità penale, civile od amministrativa;
- effettuare l'invio e l'archiviazione di messaggi di posta elettronica aventi natura oltraggiosa e/o discriminatoria o in ogni caso 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 lo stato di salute e la vita sessuale proprie e/o di terzi;
- l'invio e/o il ricevimento di allegati contenenti filmati o brani musicali (es.mp3) non legati all'attività lavorativa; l'invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list;
- la partecipazione a catene telematiche (comunemente dette "di Sant'Antonio"). Se si dovessero peraltro ricevere messaggi di tale tipo, si deve comunicarlo immediatamente al personale ITC. Non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi.

Qualora si debba conoscere il contenuto dei messaggi di posta elettronica delle caselle nome.cognome@meuccifanoli.gov.it, in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, si procederà secondo quanto previsto al p. 21 del presente Disciplinare.
L'Amministratore di Sistema, e/o i suoi incaricati, qualora ravveda situazioni particolarmente gravi e/o abusi del servizio, è tenuto ad informare la Direzione che provvederà alla contestazione delle mancanze rilevate.

7. USO DELLA RETE INTERNET E DEI RELATIVI SERVIZI

Il PC abilitato alla navigazione in Internet costituisce uno strumento dell'Istituto necessario allo svolgimento della propria attività lavorativa. È assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa.
È fatto divieto all'utente lo scarico di software gratuito (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato dall'Incaricato della gestione e manutenzione dei Sistemi Elettronici.
È tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati dalla Direzione e con il rispetto delle normali procedure di acquisto.

Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, l'Istituto IIS A. Meucci rende peraltro nota l'adozione di uno specifico sistema di blocco o filtro automatico che prevenga determinate operazioni quali *l'upload*, il *download* o l'accesso a determinati siti inseriti in una *black list*. Gli eventuali controlli, compiuti dal personale incaricato, potranno avvenire mediante un sistema di controllo dei contenuti (*Proxy server*, *Web Filtering*) o mediante "file di log" della navigazione svolta secondo quanto previsto al p. 20 del presente disciplinare.

La Direzione potrà autorizzare:

- la registrazione a siti i cui contenuti non siano legati direttamente all'attività lavorativa;
- lo scarico di *software*;
- gli acquisti on-line;
- la partecipazione a Forum non specificatamente professionali;
- l'utilizzo di *chat line*, *social network*, di bacheche elettroniche e le registrazioni in *guest books*, a fronte di specifica richiesta presentata dal Delegato responsabile;

È espressamente vietato:

- accedere ai servizi informatici Istituzionali e/o alle banche dati Istituzionali non possedendo le credenziali di accesso o mediante l'utilizzo delle credenziali di colleghi autorizzati;
- la navigazione su Social Network di qualsiasi tipo (ad es. Facebook, Twitter, Youtube, etc.), esclusi quelli espressamente approvati dalla Direzione e per soli motivi professionali;
- l'installazione, la configurazione e l'utilizzo di software "Peer-To-Peer" (P2P tipo eMule e similari) il quale, oltre a saturare le risorse di banda internet disponibili è veicolo di potenziali e gravissimi rischi per la sicurezza del sistema informatico Istituzionale nonchè può verificarsi il concreto rischio di scarico di materiale illegale (v. Legge sul Diritto d'Autore) e/o pedo-pornografico;

- la navigazione su siti appartenenti alle categorie Pedo Pornografia, Violenza, Razzismo, estremismo politico e, in generale, è espressamente vietata la navigazione e ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa;
- introdursi abusivamente in un sistema informatico o telematico protetto da misure di sicurezza contro la volontà del titolare del diritto all'accesso anche al fine di acquisire informazioni riservate;
- accedere in maniera non autorizzata ai sistemi informativi della pubblica amministrazione o alterarne in qualsiasi modo il funzionamento o intervenire con qualsiasi modalità cui non si abbia diritto su dati, informazioni o programmi contenuti in sistema informatico o telematico o a questo pertinenti, per ottenere e/o modificare informazioni a vantaggio dell'Istituto o di terzi o comunque al fine di procurare un indebito vantaggio all'Istituto od a terzi;
- distruggere, deteriorare o rendere inservibili sistemi informatici o telematici altrui, ovvero programmi, informazioni o dati utilizzati dallo Stato o da altro ente pubblico o ad esso pertinente o comunque di pubblica utilità;
- condurre, in una qualsiasi forma, attacchi telematici a terzi e/o strutture e/o strumenti digitali a loro appartenenti e, più in generale, qualsiasi azione in violazione delle leggi e delle normative vigenti in materia di Diritto della Privacy, dell'Informatica e delle Telecomunicazioni.

8. UTILIZZO DISPOSITIVI MOBILI (SMARTPHONE/TABLET)

Per "Dispositivo mobile" è da intendersi il telefono cellulare, il tablet, lo smartphone e ogni altro dispositivo che consenta la gestione di comunicazioni telefoniche, audio, video e di applicativi software "in mobilità".

In generale, i dispositivi mobili non possono essere ceduti nè fatti utilizzare a terzi, eccetto colleghi, collaboratori, consulenti o soggetti autorizzati. In particolare, alcuni telefoni sono di uso individuale e non possono essere ceduti né fatti utilizzare neppure ai colleghi.

In merito all'uso dei *device* mobili, quali strumenti di lavoro, si precisa che è proibito, senza alcuna eccezione, modificare la configurazione dei dispositivi mobili e/o installare applicazioni sospette o pirata, manualmente o da uno *store* di applicazioni (Apple Store, Google Play, ...).

Non è consentita l'installazione di ulteriori dispositivi rispetto a quelli in dotazione.

Non è consentito l'uso di qualsiasi dispositivo esterno collegabile al dispositivo mobile, se non quelli Istituzionali o quelli autorizzati.

L'utilizzatore che abbia necessità di apportare modifiche software o hardware al dispositivo mobile in dotazione, installando nuovi programmi o dispositivi, deve farne preventiva richiesta alla funzione preposta dell'Area ICT.

L'utente, ove possibile, deve mantenere aggiornato il sistema operativo e le *app* del dispositivo mobile attraverso le comuni procedure di *software update* messe a disposizione dai *Vendor*

L'utente non può forzare direttamente e/o indirettamente nè installare sul dispositivo mobile sistemi e/o software che consentano di modificarne le funzionalità, di alterarne le caratteristiche o di "prenderne il controllo" del sistema operativo (ad es.: jailbreak, root, etc…).

I dispositivi mobile devono avere abilitato il codice di blocco e/o il PIN d'accesso e/o la Password personalizzata, secondo le linee guida generali precedentemente illustrate al punto 5. Tale codice d'accesso dev'essere impostato al massimo del numero di caratteri consentito dal sistema operativo dello strumento e l'eventuale password utilizzata non deve facilmente richiamare né date di nascita né altri riferimenti anagrafici. Si consiglia l'uso di password alfanumeriche composte anche di lettere maiuscole e simboli, sempre se ammessi dal sistema operativo del mobile in dotazione. La password prescelta dovrà essere comunicata alla funzione preposta dell'Area ICT, sia al primo uso che ogni volta che si deciderà di mutarla.

Ove possibile, l'utente dovrà attivare le funzionalità di *remote wiping,* per cancellare i dati una volta che il dispositivo mobile non dovesse più essere nella disponibilità del dipendente (ad es.: casi di furto e/o smarrimento).

L'uso promiscuo dei device mobili è consentito previa autorizzazione della Direzione.

Se il dispositivo mobile consente l'attivazione dei servizi di tethering ovvero consentire la configurazione dell'apparato come gateway per offrire accesso alla Rete ad altri dispositivi che ne sono sprovvisti, questo tipo di possibilità va usata solo per periodi limitati ed in assenza di ogni altra soluzione di connettività (UMTS, WiFi, Rete Ethernet, etc.). Il servizio va immediatamente disattivato al termine dell'utilizzo e va protetto da password almeno alfanumeriche.

Il Bluetooth ed ogni altro protocollo che consenta l'associazione di dispositivi diversi dallo strumento mobile, dev'essere abilitato per l'accoppiamento ai soli strumenti Istituzionali in dotazione. Inoltre può essere usato, in particolare, per l'attivazione dell'auricolare personale e/o del kit viva-voce dell'auto. Il Bluetooth non va mai lasciato inutilmente attivo e le password d'associazione non devono mai essere quelle di default previste per il dispositivo.

E' fatto espresso divieto d'utilizzare un qualsiasi dispositivo mobile Istituzionale durante la guida. L'uso in auto è

consentito solo mediante kit "viva voce" e/o con auricolare.

L'eventuale periferica WiFi va abilitata sul dispositivo mobile solo ed esclusivamente ai fini d'accesso alla rete Istituzionale e/o di altre reti protette. Non va mai lasciato inutilmente attivo.

Del dispositivo mobile deve essere fatto regolarmente un backup o attraverso specifiche istruzioni da parte della funzione preposta dell'Area ICT.

In caso di guasti o malfunzionamenti, l'utilizzatore dovrà rivolgersi alla funzione preposta dell'Area ICT a cui è demandata la relativa gestione in queste circostanze.

La funzione preposta dell'Area ICT può disporre dei dispositivi mobile secondo necessità, sostituendo, aggiornando, rimuovendo o adeguando in tutto o in parte le componenti hardware e/o software di cui essi si compongono, senza necessità di preavviso e di richiesta di consenso da parte dell'utilizzatore.

Quanto memorizzato sui supporti interni al dispositivo mobile potrebbe essere oggetto di analisi, controllo e duplicazione da parte della funzione preposta dell'Area ICT o da personale tecnico autorizzato, per migliorare l'affidabilità, la disponibilità e l'efficienza del dispositivo.

Qualora fossero individuate componenti hardware e/o software (programmi, documenti, dispositivi esterni, etc.) non corrispondenti ai criteri di sicurezza e di operatività individuati dalla funzione preposta dell'Area ICT o non esplicitamente autorizzati, tali componenti potrebbero essere rimossi e l'utilizzatore potrebbe essere coinvolto negli accertamenti e nelle verifiche del caso.

9. OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PRIVACY

È obbligatorio attenersi alle disposizioni in materia di Privacy e di misure di sicurezza, come indicate nella lettera di designazione di incaricato del trattamento dei dati ai sensi del GDPR 2016/679.
Poiché in caso di violazioni contrattuali e giuridiche, sia l'Istituto, sia il singolo lavoratore sono potenzialmente perseguibili con sanzioni, anche di natura penale, l'Istituto verificherà, nei limiti consentiti dalle norme legali e contrattuali, il rispetto delle regole e l'integrità del proprio sistema informatico.

Ai sensi dell'art. 13 del GDPR 2016/679, in conformità a quanto disposto dalla Provvedimento n. 13 del 1° marzo 2007 dell'Autorità Garante per la privacy, si ritiene necessario informare che:

- La Direzione, attraverso L'Area ICT, effettua un monitoraggio periodico dell'hardware e del software installato nei dispositivi informatici e mobili Istituzionali. Tale operazione viene effettuata, in modo completamente automatico per i dispositivi ed i sistemi operativi che lo consentono ed in modo manuale per tutti gli altri. Il monitoraggio, necessario per finalità organizzative (inventario del parco macchine e contabilità delle licenze d'uso del software), non coinvolge in alcun modo i dati personali ed i documenti presenti sui dispositivi, ma permette la rilevazione di software installato in violazione di questo Disciplinare.
- L'Amministratore di Sistema può accedere ai dati trattati dall'utente tramite posta elettronica o navigazione in rete esclusivamente per motivi di sicurezza e protezione del sistema informatico (ad es., contrasto virus, malware, intrusioni telematiche, fenomeni quali *spamming*, *phishing*, *spyware*, etc.), ovvero per motivi tecnici e/o manutentivi e/o di regolare svolgimento dell'attività lavorativa (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione *hardware*). Fatta eccezione per gli interventi urgenti che si rendano necessari per affrontare situazioni di emergenza e massima sicurezza, il personale incaricato accederà ai dati su richiesta dell'utente e/o previo avviso al medesimo.
- Ove sia necessario per garantire la sicurezza, l'assistenza tecnica e la normale attività operativa, il personale incaricato avrà anche la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni. Lo stesso Amministratore di Sistema e/o i suoi incaricati possono, nei casi su indicati, procedere a tutte le operazioni di configurazione e gestione necessarie a garantire la corretta funzionalità del sistema informatico Istituzionale (ad es. rimozione di file o applicazioni pericolosi).
- In previsione della possibilità che , in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, si debba conoscere il contenuto dei messaggi di posta elettronica delle caselle nome.cognome@meuccifanoli.gov.it, l'utente può formalmente delegare un altro lavoratore (Fiduciario, così come definito dal Provvedimento del Garante della Privacy Nr. 13 del 1 marzo 2007 *"Lavoro: le linee guida del Garante per posta elettronica e internet"*) a verificare il contenuto dei messaggi, a gestire le strette necessità operative e/o ad inoltrare quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. In assenza della nomina di un fiduciario, da effettuarsi entro tempi adeguati per l'espletamento della richiesta avanzata da parte del Responsabile d'ufficio, con la presenza di quest'ultimo e di personale appositamente incaricato (ad esempio gli amministratori dei sistemi o i tecnici incaricati), il Titolare o persona da lui delegata, può legittimamente verificare il contenuto dei messaggi al fine da estrarre le informazioni ritenute rilevanti per lo svolgimento dell'attività lavorativa. Di tale attività verrà redatto apposito verbale e informato il lavoratore interessato alla prima occasione utile.

- Al fine di prevenire, per quanto e ove possibile, comportamenti scorretti durante la navigazione in Internet, l'Istituto si avvale di appositi filtri che impediscono l'accesso a siti non ritenuti idonei ed il download di files multimediali non attinenti all'attività lavorativa. Tali sistemi consentono anche la raccolta e la conservazione dell'attività di navigazione dei singoli utenti in appositi registri chiamati "file di log".
- L'eventuale controllo sui *file* di *log* da parte dell'Amministratore di Sistema non è comunque continuativo ed è limitato ad alcune informazioni (es. Posta elettronica: l'indirizzo del mittente e del destinatario, la data e l'ora dell'invio e della ricezione e l'oggetto – Navigazione Internet: il nome dell'utente, l'identificativo della postazione di lavoro, indirizzo IP, la data e ora di navigazione, il sito visitato e il totale degli accessi effettuati) ed i file stessi vengono conservati per il periodo strettamente necessario per il perseguimento delle finalità di sicurezza dell'Istituto, e comunque non oltre 12 mesi, fatti salvi in ogni caso specifici obblighi di legge. Il sistema di registrazione dei *log* è configurato per cancellare periodicamente ed automaticamente (attraverso procedure di sovra-registrazione) i dati personali degli utenti relativi agli accessi internet e al traffico telematico. Eventuali comportamenti anomali saranno segnalati genericamente alle aree interessate (uffici, servizi) e, solo qualora tali comportamenti dovessero continuare, la Direzione potrà procedere, nel rispetto delle norme legali e contrattuali, a controlli individuali, come previsto al p. 22 del presente Disciplinare.
- L'Amministratore di Sistema e i suoi incaricati sono altresì abilitati ad accedere ai dati contenuti negli strumenti informatici restituiti dall'utente all'Istituto per cessazione del rapporto, sostituzione delle apparecchiature, etc.

Il trattamento dei dati, così come descritto, è obbligatorio, pena l'impossibilità di utilizzare qualunque dispositivo informatico, digitale e/o mobile.
L'Istituto IIS A. Meucci garantisce la non effettuazione di alcun trattamento mediante sistemi hardware e software specificatamente preordinati al controllo a distanza.
Nell'ambito delle misure di controllo del livello di sicurezza del sistema informativo, è possibile che il Responsabile del Sistema di Gestione Sicurezza Informazioni (SGSI) o persona da lui delegata, effettui tentativi di violazione delle *password* degli utenti. Nel caso il tentativo abbia esito positivo, verrà chiesto all'utente di sostituire immediatamente la *password*.

10. SISTEMI DI CONTROLLO GRADUALI

In caso di anomalie, il personale incaricato del servizio ICT effettuerà controlli preliminari su dati aggregati, riferiti all'intera struttura lavorativa o a sue aree che si concluderanno con avvisi generalizzati diretti ai dipendenti di detta struttura o aree in cui sia stata rilevata l'anomalia, nei quali si evidenzierà l'utilizzo irregolare degli strumenti Istituzionali e si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite. Controlli su base individuale potranno essere compiuti solo in caso di successive ulteriori anomalie (come previsto dal p. 6.1 della Delibera Nr. 13 del 1/3/2007 Garante Privacy *"Lavoro: le linee guida del Garante per posta elettronica e internet"*).
In alcun caso verranno compiuti controlli prolungati, costanti o indiscriminati.

11. NON OSSERVANZA DEL PRESENTE REGOLAMENTO

Il mancato rispetto o la violazione delle regole contenute nel presente regolamento è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali consentite.

12. AGGIORNAMENTO E REVISIONE

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento. Le proposte verranno esaminate dalla Direzione.
Il presente Regolamento è soggetto a revisione con frequenza annuale.

Cittadella, 02/10/2018

l'Istituto IIS A. Meucci