COMUNE DI TRECENTA

DELIBERAZIONE DELLA GIUNTA COMUNALE N. 102 DEL 23/09/2019

OGGETTO: Linee Guida per l'attuazione del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali

L'anno duemiladiciannove, addì ventitre, del mese di Settembre, alle ore 17:30, presso la SEDE DELLA GIUNTA, previo esaurimento delle formalità prescritte dalla Legge dello Stato e dallo Statuto, si è riunita la Giunta Comunale sotto la presidenza del Sindaco Sig. LARUCCIA ANTONIO.

All'appello nominale risulta:

CARICA	COGNOME E NOME	PRESENTE
SINDACO	LARUCCIA ANTONIO	SI
VICE SINDACO	TEGAZZINI MATTEO	SI
ASSESSORE ESTERNO	BISAGLIA SIMONA	SI

Presenti n° 3 Assenti n° 0

Partecipa il Segretario Comunale Dott. CIRILLO GIOVANNI, il quale provvede alla redazione del presente verbale.

Essendo legale il numero degli intervenuti, il Sig. LARUCCIA ANTONIO, nella sua qualità di Sindaco, assume la presidenza e dichiara aperta la seduta per la trattazione dell'oggetto sopra riportato.

LA GIUNTA COMUNALE

Richiamata la deliberazione di Giunta Comunale n. 93 del 10 luglio 2018, con la quale il Comune ha adeguato la propria modulistica alla nuova normativa in materia di tutela della riservatezza delle persone fisiche con riguardo al trattamento dei dati personali di cui al Reg. UE 679/2016;

Ravvisata la necessità di intervenire nuovamente sulla materia *de qua*, anche alla luce dei mutamenti legislativi intervenuti nel corso dell'ultimo anno nonché sulla base dei pareri in materia rilasciati dall'Autorità Garante per la Privacy;

Preso atto più nello specifico della necessità di impartire delle direttive quanto all'uso delle apparecchiature telematiche, informatiche messe a disposizione dal Comune, e comunque più in generale quanto all'uso degli strumenti di lavoro, in un'ottica di garanzia della privacy degli stessi incaricati nonché dei fruitori dei servizi;

Considerata meritevole di approvazione la documentazione allegata;

Acquisito il parere favorevole in ordine alla sola regolarità tecnica di cui all'art 49, comma 1 del D.Lgs n.267/2000 espresso dal responsabile interessato;

Con votazione unanime e favorevole espressa nelle forme di legge;

DELIBERA

1. di considerare quanto esposto in premessa parte integrante del presente atto;
2. di approvare le Linee Guida allegate al presente atto;
3. di disporre la pubblicazione della documentazione di cui ai punto 2 in amministrazione trasparente disposizioni generali, nonché nella sezione privacy presente nella home page del Comune.

Considerata poi l'urgenza di provvedere in considerazione dell'esigenza di conformarsi pienamente alla normativa riguardante la tutela della riservatezza delle persone fisiche e il trattamento dei dati personali, con separata votazione unanime e favorevole espressa nelle forme di legge .

DELIBERA

Di considerare il presente atto immediatamente eseguibile ex art. 134, comma 4, d. lgs. 267/2000.

PARERE DI REGOLARITA' TECNICA

Il Responsabile del Servizio ai sensi dell'art. 147/bis del TUEL 267/2000 e dell'art. 11 del Regolamento sui controlli interni in ordine alla proposta **n.ro 576 del 21/09/2019** esprime parere **FAVOREVOLE.**

Parere firmato dal Responsabile del Servizio **SPIRANDELLI SIMONE** in data **23/09/2019**

LETTO FIRMATO E SOTTOSCRITTO

Il Sindaco	Il Segretario Comunale
Sig. LARUCCIA ANTONIO	Dott. CIRILLO GIOVANNI

NOTA DI PUBBLICAZIONE N. 939

Ai sensi dell'art. 124 del T.U. 267/2000 il Responsabile della Pubblicazione **STELLA FRANCESCA** attesta che in data **14/10/2019** si è proceduto alla pubblicazione sull'Albo Pretorio.

La Delibera è esecutiva ai sensi delle vigenti disposizione di legge

LINEE GUIDA

Comune di TRECENTA

Versione	
Data Approvazione	
Responsabile	

1. Perché le Linee Guida?

La diffusione delle nuove tecnologie informatiche ed in particolare l'utilizzo della rete internet tramite le risorse informatiche e l'aumento di informazioni trattate con strumenti elettronici aumentano di fatto i rischi legati alla sicurezza e all'integrità delle informazioni oltre alle conseguenti responsabilità previste dalla normativa civile e penale.
Il Comune di Trecenta (nel seguito Ente), pertanto, deve provvedere a garantire la continuità della sua attività e assicurare la riservatezza delle informazioni e dei dati, in maniera tale da evitare che comportamenti consapevoli e/o inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati o diminuire l'efficienza delle risorse informatiche dell'Ente.
In questo contesto, l'Ente ha ritenuto necessario adottare le presenti Linee Guida al fine di evidenziare ai propri dipendenti e collaboratori le indicazioni e le misure necessarie e opportune per il corretto utilizzo nel rapporto di lavoro dei personal computer (fissi e portatili), della posta elettronica e di internet inclusi social network, definendo le modalità di utilizzo nell'ambito dell'attività lavorativa e dando la massima diffusione alla cultura sulla sicurezza informatica intesa come capacità e consapevolezza dell'utilizzo delle risorse informatiche.

2. Principi generali

Con l'approvazione delle presenti Linee Guida l'Ente si pone l'obiettivo di fornire a tutti i dipendenti le linee di comportamento per il corretto utilizzo delle risorse informatiche, della posta elettronica e dell'accesso alla rete internet.
Inoltre, l'Ente, in qualità di Titolare del trattamento dei dati personali, ritiene opportuno dotarsi di queste Linee Guida al fine di adempiere gli obblighi fissati dalle Linee Guida Europeo sul trattamento dei dati personali (GDPR).

I trattamenti effettuati dall'Ente rispettano le garanzie poste in essere dal legislatore in materia di protezione dei dati personali e si svolgono nell'osservanza dei principi sanciti dalla normativa privacy.
In quest'ottica, l'Ente tratta i dati dei lavoratori nella misura meno invasiva possibile, affidando eventuali attività di monitoraggio esclusivamente a quei soggetti opportunamente preposti ed effettuando eventuali controlli esclusivamente in maniera mirata sull'area di rischio.
Ogni lavoratore potrà far valere i propri diritti sanciti dalla normativa sul trattamento dei dati personali rivolgendo una specifica richiesta scritta al Titolare del trattamento.

2.1. Campo di applicazione

Le presenti Linee Guida si applicano a tutti i lavoratori ed a tutti i collaboratori dell'Ente, a prescindere dal rapporto contrattuale con la stessa intrattenuto (lavoratori somministrati, collaboratori a progetto, stagisti, consulenti ecc…).
Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "Utente" deve intendersi ogni dipendente e collaboratore (collaboratore a progetto, in stage, agente, ecc.) in possesso di specifiche credenziali di autenticazione e autorizzato all'utilizzo delle risorse informatiche ed al trattamento dei dati personali.

2.2. Entrata in vigore e Aggiornamenti

Le Linee Guida sono state approvate con delibera di G.C. n 93 del 10.07.2018 e sarà adottato dal Comune di Trecenta. Con l'entrata in vigore delle presenti Linee Guida tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalle presenti.

Al fine di informare i propri dipendenti del contesto delle presenti Linee Guida le stesse saranno:

a) consegnate a ciascun dipendente ed a ciascun collaboratore ad inizio attività.
b) affisse nella bacheca aziendale

L'Ente si riserva la facoltà di apportare, in qualsiasi momento, modifiche al presente documento, dandone comunicazione a tutti gli incaricati con le modalità che riterrà opportune.
Le presenti Linee Guida sono state predisposte ad uso esclusivamente interno dell'Ente e, pertanto, non potrà essere riprodotto, divulgato, copiato, utilizzato e/o altrimenti reso pubblico in assenza di una previa approvazione scritta dell'Ente stesso.

3. Regole di comportamento generali

Il Comune di Trecenta è titolare di qualsiasi diritto connesso ai sistemi informativi ed alle risorse informatiche, ai dati, ai contenuti di ogni tipo e genere, elaborati, creati, o modificati nell'ambito delle attività lavorative e tramite l'opera dei suoi dipendenti e collaboratori.
Per **Risorse informatiche** si intende qualsiasi strumento informatico di proprietà dell'Ente ed utilizzato dal lavoratore per rendere la prestazione lavorativa. A titolo esemplificativo ma non esaustivo sono risorse informatiche: personal computer fissi e portatili; tablets; telefoni cellulari semplici; telefoni cellulari smartphone; viacard; telepass; carte di credito; sistemi di geolocalizzazione (navigazione satellitare e sistemi di antifurto satellitare) installati su veicoli aziendali, indirizzo e-mail aziendale, rete aziendale.
L'utilizzo delle risorse informatiche e telematiche aziendali, deve avvenire nell'ambito del generale contesto di diligenza, fedeltà e correttezza che caratterizza il rapporto lavorativo fra l'Ente ed i propri dipendenti. L'Utente dovrà adottare tutte le cautele e le precauzioni necessarie per evitare le possibili conseguenze dannose alle quali un utilizzo non avveduto di tali strumenti può produrre, anche in considerazione della difficoltà di tracciare una netta linea di confine tra l'attività lavorativa e la sfera personale e la vita privata del lavoratore e di terzi che interagiscono con quest'ultimo.
L'Ente, pertanto, consapevole delle potenzialità fornite dagli strumenti informatici e telematici, li mette a disposizione dei propri dipendenti e collaboratori esclusivamente per finalità di tipo lavorativo.
Non è quindi permesso utilizzare, tranne espressa autorizzazione, detti strumenti per altre finalità non connesse all'attività lavorativa o in modo che violino qualsiasi disposizione normativa.
Al riguardo si evidenzia che l'Ente adotterà ogni accorgimento tecnico necessario a tutelarsi da eventuali comportamenti non permessi, salvaguardano il rispetto della libertà e della dignità dei lavoratori.

Di seguito vengono descritte le linee di comportamento a cui gli Utenti devono attenersi nell'esecuzione dei compiti che implicano un trattamento di dati personali tramite le risorse informatiche.
In generale l'Utente deve osservare le seguenti regole di ordinaria diligenza, nonché tutte le altre ulteriori misure ritenute necessarie per garantire il rispetto di quanto disposto dalla normativa privacy:

a) tutte le operazioni di trattamento devono essere effettuate in modo tale da garantire il rispetto delle misure di sicurezza, la massima riservatezza delle informazioni di cui si viene in possesso considerando tutti i dati confidenziali e, di norma, soggetti al segreto d'ufficio;
b) le singole fasi di lavoro e la condotta da osservare devono consentire di evitare che i dati siano soggetti a rischi di perdita o distruzione, che vi possano accedere persone non autorizzate, che vengano svolte operazioni di trattamento non consentite o non conformi ai fini per i quali i dati stessi sono stati raccolti;
c) non devono essere eseguite operazioni di trattamento per fini non previsti tra i compiti assegnati dal diretto responsabile;
d) devono essere svolte le sole operazioni di trattamento necessarie per il raggiungimento dei fini per i quali i dati sono stati raccolti;
e) deve essere costantemente verificata l'esattezza dei dati trattati e la pertinenza rispetto alle finalità perseguite nei singoli casi.

Quanto sopra descritto impone, in altri termini, all'Utente di operare con la massima attenzione in tutte le fasi di trattamento, dalla esatta acquisizione dei dati, al loro aggiornamento, alla conservazione ed eventuale distruzione.

4. Regole operative

4.1 Uso del Pc

Il personal computer (comprese le periferiche ad esso connesse) ed i relativi programmi e/o applicazioni affidati al dipendente sono, come è noto, strumenti di lavoro; tali strumenti pertanto:

a) vanno custoditi in modo appropriato;
b) possono essere utilizzati solo per fini professionali (in relazione, ovviamente, alle mansioni assegnate) e non a fini personali, tanto meno per scopi illeciti; Ogni utilizzo non inerente all'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione. Eventuali minacce alla sicurezza (ad esempio mail di phishing, spam, virus) devono essere prontamente segnalate all'azienda, come anche il furto, il danneggiamento, lo smarrimento.
c) Il personal computer dato in affidamento all'Utente permette l'accesso alla rete dell'Ente solo attraverso specifiche credenziali di autenticazione**.**
d) Non è consentito l'uso di programmi diversi da quelli ufficialmente installati dell'Ente né viene consentito agli utenti di installare autonomamente programmi provenienti dall'esterno, sussistendo infatti il grave pericolo di introdurre Virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti.

e) Non è consentita la riproduzione o la duplicazione di programmi informatici ai sensi della Legge 21/05/2004 n. 128. L'inosservanza della presente disposizione espone lo stesso Ente a gravi responsabilità civili; si evidenzia, inoltre, che le violazioni della normativa a tutela dei diritti d'autore sul software che impone la presenza nel sistema di software regolarmente licenziato, o comunque libero e quindi non protetto dal diritto d'autore, vengono sanzionate penalmente e possono anche comportare il sorgere di una responsabilità amministrativa a carico dell'Ente.
f) Non è consentita l'attivazione della password d'accensione (Bios) senza preventiva autorizzazione dell'amministratore di sistema, né modificare le caratteristiche hardware e software impostate sul proprio PC, né procedere ad installare dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, hard disk esterni, chiavette usb, o comunque supporti di memorizzazione in genere considerati esterni), salvo previa autorizzazione esplicita da parte dell'amministratore di sistema.
g) Ogni Utente deve prestare la massima attenzione ai supporti di origine esterna (supporti usb), avvertendo immediatamente l'Amministratore di Sistema nel caso in cui siano rilevati virus.
h) Ogni Utente dovrà effettuare i salvataggi dei file su server evitando di effettuare salvataggi sul disco rigido del PC o su supporti di archiviazione removibili. Particolare attenzione deve essere prestata alla duplicazione dei dati. E' infatti da evitare l'archiviazione ridondante.
i) Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio o in caso di suo inutilizzo. 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**. In ogni caso è buona norma attivare lo screensaver con password anche in assenza per piccoli periodi.**

4.2 Utilizzo di Pc Portatili

L'Utente è responsabile del PC portatile assegnatogli dall'Ente e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.
I PC portatili:
□ utilizzati all'esterno dell'Ente, devono essere custoditi con diligenza, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni.
□ non devono essere lasciati incustoditi e sul disco devono essere conservati solo i file strettamente necessari.
Nel caso di accesso alla rete aziendale tramite RAS (Remote Access Server) / Accesso Remoto / VPN (Virtual Private Network), deve essere utilizzato l'accesso in forma esclusivamente personale attraverso le Credenziali di Autenticazione alla rete. Al termine della sessione di collegamento, dovrà essere effettuata la disconnessione attraverso il software utilizzato.
I PC portatili, dovranno essere periodicamente collegati alla Rete interna al fine di consentire gli aggiornamenti antivirus.

Ai fini dei collegamenti alla rete internet, è vietato l'utilizzo di abbonamenti internet privati e relativi hardware di connessione (chiavette, data card ecc.).

Uso dei dischi di rete (directory)

Si conferma l'obbligatorietà del salvataggio dei dati sulle apposite unità di rete messe a disposizione dell'utenza la fine di evitare perdite dati ed agevolare le operazioni di backup degli stessi.

4.3. Credenziali di autenticazione

Le credenziali di autenticazione per l'accesso al PC, la connessione alla rete e/o per l'accesso ai diversi applicativi, vengono assegnate all'Utente dall'Amministrazione di sistema, in seguito alla sottoscrizione del contratto di assunzione o di collaborazione.
Le credenziali di autenticazione consistono in un codice per l'identificazione dell'Utente (user id), associato ad una parola chiave (password) riservata che dovrà venir custodita dall'Utente con la massima diligenza e non divulgata.
La password, che rappresenta la parte segreta delle credenziali, è conosciuta solo dall'Utente, è composta da almeno da 8 caratteri, può essere formata da lettere (maiuscole o minuscole) e/o numeri, anche in combinazione fra loro, e non contiene riferimenti facilmente riconducibili all'Utente (nome, cognome, data di nascita ecc.).
L'utente ha l'obbligo di modificare la password dopo il primo utilizzo e poi modificata con cadenza trimestrale.
Per garantire la segretezza delle credenziali e la sicurezza durante le sessioni di trattamento dei dati, ogni Utente dovrà:
a) Evitare di condividere in qualsiasi modo la password;
b) Non lasciare accessibile l'elaboratore durante una sessione di trattamento dei dati;
c) Impostare uno screen saver dotato di password (con tempi di avvio brevi) che blocchi l'accesso all'elaboratore in caso sia necessario allontanarsi per un tempo prolungato;
d) Qualora l'elaboratore sia utilizzato da più incaricati, ricordarsi, sempre al termine del lavoro effettuato, di disconnettersi dal sistema (dal menu avvio/start scegliere chiudi e poi disconnetti Utente).
Le credenziali sono strettamente personali e non possono essere cedute a terzi. Il mantenimento della segretezza delle credenziali è ad esclusivo carico dell'Utente, il quale sarà il solo responsabile per qualsiasi attività posta in essere tramite l'utilizzo delle stesse.

4.4. Uso antivirus

Il sistema informatico ed i pc collegati alla rete dell'Ente sono protetti da software antivirus aggiornati quotidianamente automaticamente.
È vietato cancellare, riconfigurare o disattivare detto software antivirus.
Ogni Utente è comunque tenuto a comportarsi in modo tale da ridurre il rischio di attacco al sistema informatico aziendale da parte di virus o attraverso qualsiasi altro software "aggressivo".
L'Utente dovrà segnalare eventuali anomalie all'amministratore di sistema o altro referente dell'Ente:

□ qualora vi sia motivo di ritenere che il pc sia stato infettato o che non sia installata l'ultima versione aggiornata dell'antivirus, bisogna immediatamente segnalarlo;
□ nel caso di riconoscimento di virus, il sistema proporrà un messaggio di avviso, e nei rari casi in cui il sistema antivirus non fosse in grado di rimuovere il virus;
L'Utente è tenuto ad una verifica periodica manuale dei propri dischi locali attivando la scansione antivirus.

4.5 Utilizzo e Conservazione dei supporti rimovibili

Tutti i supporti magnetici rimovibili (dischetti, CD e DVD riscrivibili, supporti USB, ecc.), contenenti dati personali e/o informazioni costituenti know-how aziendale, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato. L'Utente è responsabile della custodia dei supporti e dei dati aziendali in essi contenuti.
Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati personali, ciascun Utente dovrà contattare l'amministratore di sistema e seguire le istruzioni da questo impartite.
In ogni caso, i supporti magnetici contenenti dati personali devono essere dagli Utenti adeguatamente custoditi in armadi chiusi.
E' vietato l'utilizzo di supporti rimovibili personali.

4.6. Utilizzo dei device (smartphone - tablet)

I device affidati all'Utente sono strumenti di lavoro e l'Ente non ne consente un utilizzo promiscuo. Gli utilizzi non strettamente inerenti all'attività lavorativa dovranno essere comunque limitati e regolati da un minimo di diligenza. Rimane inteso che è assolutamente vietato l'utilizzo dei device forniti per la visione, il download ed il caricamento di contenuti contrari al buoncostume e rientranti quindi in ambiti pornografici e/o violenti; altresì vietato il download, la riproduzione e la condivisione di contenuti online e multimediali ottenuti illegalmente in violazione alla normativa sul diritto d'autore ed al codice penale.
Ogni utilizzo che possa in qualche modo contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza, è assolutamente vietato; qualora si riscontrassero addebiti o sanzioni derivanti da un utilizzo improprio del device questi rimarranno a carico della persona che ha commesso l'infrazione.

I device devono essere custoditi con cura evitando ogni possibile forma di danneggiamento. L'Utente è responsabile dei device assegnati e deve custodirli con diligenza sia fuori dall'Ente sia durante l'utilizzo nel luogo di lavoro.
I device utilizzati fuori dalla sede dell'Ente, devono essere custoditi con diligenza, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni.

4.7 Uso della rete aziendale

Per l'accesso alla rete dell'Ente ciascun Utente deve essere in possesso della specifica Credenziale di Autenticazione (username e password).
È assolutamente proibito entrare nella rete e nei programmi con un codice d'identificazione Utente diverso da quello assegnato. Le password d'accesso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite.

Le cartelle utenti presenti nei server dell'Ente 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 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 back up da parte dell'Amministratore di Sistema.
Si ricorda che tutti i dischi o altre unità di memorizzazione locali (es. disco C: interno PC) non sono soggette a salvataggio da parte del personale incaricato dell'Amministratore di sistema. La responsabilità del salvataggio dei dati ivi contenuti è pertanto a carico del singolo Utente.
È vietato connettere in rete stazioni di lavoro o altri dispositivi hardware, se non previa autorizzazione dall'Ente. È vietato monitorare, attraverso qualsiasi dispositivo hardware o software, ciò che transita in rete. È vietata l'installazione non autorizzata di modem che sfruttino il sistema di comunicazione telefonica per l'accesso a banche dati esterne o interne all'azienda.
L'Amministratore di Sistema può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza sia sui PC degli Utenti sia sulle unità di rete.
Risulta opportuno che, con regolare periodicità (almeno ogni tre mesi), ciascun Utente provveda alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.

4.8 Uso della rete internet

La rete Internet è ormai divenuta uno strumento operativo di comunicazione imprescindibile pertanto costituisce a tutti gli effetti uno strumento aziendale necessario allo svolgimento dell'attività lavorativa.
Un suo utilizzo indiscriminato, però, può rendere la Società vulnerabile sotto il profilo della sicurezza. È quindi assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa.

Pertanto, l'Utente deve usare Internet in modo da non rivelare o diffondere al pubblico informazioni di tipo confidenziale o di proprietà dell'azienda (es. informazioni finanziarie, nuovi progetti di business e produzione, piani e strategie di marketing, database ed informazioni in essi contenute, liste clienti, informazioni tecniche di prodotto, software, codici di accesso ai computer ed alla rete, dati ed informazioni personali e relazioni di lavoro);

Alla luce di ciò, l'Ente, anche per limitare il più possibile i controlli, ha adottato alcune misure ritenute opportune per proteggere i propri sistemi elettronici dall'eventuale utilizzo non accorto della navigazione su Internet da parte dei lavoratori.

In particolar modo gli utenti non possono utilizzare strumenti privati per il collegamento alla rete. In questo senso, a titolo puramente esemplificativo, l'Utente non potrà utilizzare internet per:

a) l’upload o il download di software gratuiti (freeware) e shareware, nonché l’utilizzo di documenti provenienti da siti web o http, se non strettamente attinenti all’attività lavorativa (filmati e musica) e previa verifica dell’attendibilità dei siti in questione;
b) l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, fatti salvi i casi direttamente autorizzati dall’Ente e comunque nel rispetto delle normali procedure di acquisto;
c) ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa;
d) la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche come i social network e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames) se non espressamente autorizzati dall’Ente;
e) l’accesso, tramite internet, a caselle webmail di posta elettronica personale.

Al fine di evitare la navigazione in siti non pertinenti (a rischio) all’attività lavorativa, l’Ente rende peraltro noto (obbligatoria) l’adozione di uno (specifico) sistema di blocco o filtro automatico che prevengano determinate operazioni quali l’upload o l’accesso a siti ad alta rischiosità inseriti in una black list.
I filtri sopraindicati limitano l’accesso ai siti Internet che presentano i seguenti contenuti:
□ illegali o non etici;
□ materiale per adulti, pornografia;
□ giochi, scommesse, intermediazione e trading, download software;
□ social network, radio e tv internet;
□ peer to peer;
□ malware, spyware, hacking, bypass proxy, phishing.
Gli eventuali controlli, compiuti dall’Amministratore di Sistema potranno avvenire mediante un sistema di controllo dei contenuti (Proxy server) o mediante “file di log” della navigazione svolta. Il controllo sui file di log non è continuativo ed i file stessi vengono conservati non oltre il tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza dell’azienda.

4.9 Uso della posta elettronica

La casella di posta elettronica assegnata all'Utente è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.
È vietato utilizzare le caselle di posta elettronica **nome.cognome@comune.sanbellino.ro.it** o quelle condivise tra più utenti 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 per:
a) l’invio e/o il ricevimento di allegati contenenti filmati o brani musicali (es.mp3) non legati all’attività lavorativa;
b) l’invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list se non legati all’attività lavorativa;

c) la partecipazione a catene telematiche (o di Sant'Antonio). Se si dovessero peraltro ricevere messaggi di tale tipo, si deve comunicarlo immediatamente all'Amministratore di Sistema. Non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi.
La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.
Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per l'Ente ovvero contenga documenti da considerarsi riservati in quanto contraddistinti dalla dicitura "strettamente riservati" o da analoga dicitura, deve essere visionata od autorizzata dalla Direzione.
Nel caso di mittenti sconosciuti o messaggi insoliti, per non correre il rischio di essere infettati da virus, occorrerà cancellare i messaggi senza aprirli. (Conosciute come tecniche intrusive di Spamming e phishing)
Nel caso di messaggi provenienti da mittenti conosciuti ma che contengono allegati sospetti (file con estensione .exe, .scr, .bat ecc), oppure o file che abbiamo nomi simili a documenti che comunque hanno estensione ZIP o diano parvenza di archivio compresso non devono essere aperti. È obbligatorio quindi porre la massima attenzione nell'aprire i file attachements di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).
In caso di assenza dell'Utente si potrà delegare altro Utente precedentemente identificato a verificare il contenuto dei messaggi ed a gestire quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Sarà comunque consentito all'Amministratore di sistema accedere alla casella di posta elettronica dell'Utente, in caso di assenza, qualora si renda necessario. Di tale operazione deve essere data comunicazione all'Utente titolare della casella di posta.
Al fine di ribadire agli interlocutori la natura esclusivamente aziendale della casella di posta elettronica, i messaggi devono contenere un avvertimento standardizzato nel quale sia dichiarata la natura non personale dei messaggi stessi.
Al fine di garantire la funzionalità del servizio di posta elettronica aziendale e di ridurre al minimo l'accesso ai dati, nel rispetto del principio di necessità e di proporzionalità, il sistema, in caso di assenze programmate (ad es. per ferie o attività di lavoro fuori sede dell'assegnatario della casella) invierà automaticamente messaggi di risposta contenenti le "coordinate" di posta elettronica di un altro soggetto o altre utili modalità di contatto della struttura. In tal caso, la funzionalità deve essere attivata dall'Utente.
In caso di assenza non programmata (ad es. per malattia) la procedura - qualora non possa essere attivata dal lavoratore avvalendosi del servizio webmail entro due giorni - verrà attivata a cura dell'Ente.

4.10 Uso stampanti

Per quanto concerne l'utilizzo delle stampanti, gli utenti sono tenuti a:
□ stampare documenti e atti solo se strettamente necessari per lo svolgimento delle proprie funzioni lavorative;
□ prediligere le stampanti di rete in luogo di quelle locali al fine di ridurre l'utilizzo di materiali di consumo;
□ le stampanti locali devono essere spente ogni sera prima di lasciare gli uffici o in caso di loro utilizzo.

Qualora l'Utente dovesse stampare documenti contenenti dati o informazioni riservate, dovrà avere cura di monitorare la stampante e preservare, limitatamente alle oggettive possibilità, la conoscibilità di tali dati o informazioni da parte di terzi non autorizzati.

4.11 Gestione dati

L'Ente raccomanda di salvare frequentemente i documenti su cui si lavora ed in particolare, quando ci si allontana dalla postazione anche per breve tempo.
Costituisce buona regola la periodica pulizia degli archivi, con cancellazione dei file obsoleti o che hanno alcuna finalità e/o utilità per il business aziendale o perché non utilizzabili, o non più utilizzabili, per le attività/funzioni/mansioni assegnate. Particolare attenzione deve essere prestata alla duplicazione dei dati. E', infatti, assolutamente da evitare un'archiviazione ridondante.
I dipendenti e collaboratori devono salvare i dati ed i documenti aziendali nell'eventuale sistema documentale.
Il disco rigido di ogni PC, infatti, è destinato a contenere solo il software per il funzionamento della macchina e per la produttività individuale.

Misure organizzative

Si conferma l'obbligatorietà del salvataggio dei dati sulle apposite unità di rete messe a disposizione dell'utenza la fine di evitare perdite dati ed agevolare le operazioni di backup degli stessi.

5. Monitoraggi e controlli dell'Ente

5.1 Accesso Ai Dati Dell'Utente

L'Amministratore di Sistema o i suoi delegati possono 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).
L'Amministratore di Sistema, in caso di assenza improvvisa o prolungata dell'Utente o comunque non programmata e per improrogabili necessità di sicurezza o di operatività del sistema è abilitato ad accedere alla posta elettronica dell'Utente per le strette necessità operative. Di tale avvenuto accesso dovrà comunque essere data tempestiva comunicazione all'Utente.
L'Amministratore di Sistema può procedere a controlli sulla navigazione finalizzati a garantire l'operatività e la sicurezza del sistema, nonché il necessario svolgimento delle attività lavorative, es. mediante un sistema di controllo dei contenuti (Proxy server) o mediante "file di log" della navigazione svolta.
Il sistema informativo fornisce una serie di informazioni inerenti l'utilizzo dei software e/o dell'hardware di ciascuna postazione di lavoro. In via esemplificativa e non esaustiva il sistema informativo fornisce:
□ log di accesso a internet;
□ log inerenti la posta elettronica e servizi mail to fax;

□ log inerenti l'accesso alle banche dati e agli applicativi;
□ log inerenti la telefonia;
□ log inerenti alle attività eseguite;
□ log di attività di computer (accensione, spegnimento);
□ log di stampa.

L'eventuale controllo sui file di log da parte dell'Amministratore di Sistema non è comunque continuativo ed è limitato ad alcune informazioni, ad esempio:

a) Posta elettronica: l'indirizzo del mittente e del destinatario, la data e l'ora dell'invio e della ricezione e l'oggetto.
b) 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.

I file di Log vengono conservati per il periodo strettamente necessario per il perseguimento delle finalità organizzative, produttive e di sicurezza dell'azienda, e comunque non oltre 6 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 sovrascrittura) i dati personali degli utenti relativi agli accessi internet e al traffico telematico.
L'Amministratore di Sistema è altresì abilitato ad accedere ai dati contenuti negli strumenti informatici restituiti dall'Utente all'azienda per cessazione del rapporto, sostituzione delle apparecchiature, etc.
Sarà cura dell'Utente la cancellazione preventiva di tutti gli eventuali dati personali eventualmente ivi contenuti.
In ogni caso, l'Ente garantisce la non effettuazione di alcun trattamento mediante sistemi hardware e software specificatamente preordinati al controllo a distanza, quali, a titolo esemplificativo:
a) lettura e registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori (log) al di là di quanto tecnicamente necessario per svolgere il servizio e-mail;
b) riproduzione ed eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore;
c) lettura e registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo.

Controlli

L'Ente ha l'obbligo di salvaguardare la funzionalità e il corretto impiego degli strumenti informatici da parte dei lavoratori, pertanto, si riserva il diritto di effettuare controlli per verificare il rispetto delle presenti Linee Guida.
A tale proposito si sottolinea che le Risorse Informatiche sono di proprietà dell'Ente in quanto mezzo di lavoro. È pertanto fatto divieto di utilizzo delle Risorse Informatiche e dell'accesso alla rete internet per fini ed interessi non strettamente coincidenti con quelli dell'Ente stesso.
Con riferimento a tali controlli le presenti Linee Guida costituiscono preventiva e completa informazione nei confronti dei dipendenti e collaboratori.

Le verifiche sugli strumenti informatici saranno eseguite dall'Ente nel pieno rispetto dei diritti e delle libertà fondamentali degli utenti e delle presenti Linee Guida, secondo i principi di pertinenza e non eccedenza.
L'Ente, pertanto, si riserva il diritto di controllare, anche in maniera occasionale e/o discontinua il corretto utilizzo degli strumenti di lavoro, implementando, però, ogni misura tecnologica volta a minimizzare il più possibile l'uso di dati identificativi dei lavoratori, nei modi e nei limiti esplicitati di seguito e nel successivo paragrafo denominato "Graduazione dei controlli".

In nessun caso tali controlli verranno impiegati per un monitoraggio dell'efficienza dell'attività lavorativa del singolo individuo come prescritto dall'art. 4 Statuto dei lavoratori.

I controlli si svolgeranno in forma graduata:

a) in via preliminare l'Ente provvederà ad eseguire dei controlli su dati aggregati, riferiti all'intera struttura ovvero a sue aree e dunque un controllo anonimo che può concludersi con un avviso generalizzato relativo ad un rilevato utilizzo anomalo degli strumenti aziendali e con invito ad astenersi scrupolosamente ai compiti assegnati ad alle istruzioni impartite;
b) in assenza di successive anomalie non si effettueranno controlli su base individuale. In tali casi, il controllo si concluderà con un avviso ai dipendenti interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.

Nel caso vengano rilevate continue anomalie si procederà a controlli su base individuale o per postazione di lavoro e in caso di abusi di singoli e reiterati si eseguiranno controlli nominativi o su singoli dispositivi e/o postazioni di lavoro (indicando le ragioni legittime, specifiche e non generiche, per cui i controlli vedrebbero effettuati – anche per verifiche sulla funzionalità e di sicurezza del sistema – inoltrando preventivi avvisi collettivi o individuali).

Le attività sull'uso del servizio di accesso ad Internet vengono automaticamente registrate in forma elettronica attraverso i c.d. "log di sistema". Questi sistemi software sono programmati e configurati in modo da cancellare periodicamente e automaticamente, attraverso procedure di sovrascrittura dei log file, i dati personali relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia più necessaria.

Oltre che per motivi di sicurezza del sistema informatico, anche per motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.) o per finalità di controllo e programmazione dei costi aziendali (ad esempio, verifica costi di connessione ad Internet, traffico telefonico, etc.), comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è facoltà dell'Ente, tramite il personale del Servizio IT o addetti alla manutenzione, accedere direttamente, nel rispetto della normativa sulla privacy, a tutti gli strumenti informatici aziendali ed ai documenti ivi contenuti, nonché alle caselle email ed ai tabulati del traffico telefonico.

Violazioni e sanzioni disciplinari

È fatto obbligo a tutti gli utenti di osservare le disposizioni portate a conoscenza con le presenti Linee Guida. Il mancato rispetto o la violazione delle regole sopra ricordate è perseguibile nei confronti del personale dipendente con i provvedimenti disciplinari previsti dalla normativa vigente e dai regolamenti interni; nonché con le azioni civili e penali previste dalla normativa di riferimento.